دليل التحقق

من عمليات التضليل والتلاعب الإعلامي

آليات التحقق على المنصات الرقمية والتحرّي
عن حسابات التواصل الاجتماعي للكشف عن الأنشطة الموجّهة
وعمليات التلاعب بالمحتوى



European Journalism Centre

تحرير **كريغ سيلفرمان**

معهد
الجزيرة للإعلام

تَرجم هذا الكتاب إلى اللغة العربية
معهد الجزيرة للإعلام
بالتعاون مع مركز الصحافة الأوروبي

الطبعة الأولى
معهد الجزيرة للإعلام 2020

الرقم الدولي (ردمك):
978-605-06798-2-3

دليل التحقق من عمليات التضليل والتلاعب الإعلامي

آليات التحقق على المنصات الرقمية والتحرّي عن حسابات التواصل
الاجتماعي للكشف عن الأنشطة الموجّهة وعمليات التلاعب بالمحتوى

Verification Handbook
for Disinformation and Media Manipulation

A definitive guide for investigating platforms and online accounts to
reveal inauthentic activity and manipulated content

تحرير
كريغ سيلفرمان

تحرير النسخة العربية
منتصر مرعي
محمد خمايسة

ترجمة
محمد زيدان

تدقيق لغوي
د. سليمان العميرات

تصميم النسخة العربية
أحمد فتاح

الفهرس

الفصل العاشر:

الفصل الحادي عشر:

مقدمة الطبعة العربية

بين عامي 2019-2020، نشر «رافايل باداني Raphael Badani»، الخبير في شؤون الشرق الأوسط، مجموعة من المقالات والتحليلات حول الشرق الأوسط في عدد من المواقع الصحفية اليمينية الأميركية. لم يكن باداني سوى شخصية وهمية، ضمن شبكة دعاية مكونة من 19 شخصية، استخدمت تقنيات متطورة لإخفاء هويتها الأصلية، ونشرت مقالات وتحليلات تروّج لوجهة نظر تدعم دولة الإمارات وتنتقد سياسات قطر وتركيا وإيران، حسب تحقيق لموقع The Daily Beast الأميركي.

سعت هذه الحملة، وغيرها من حملات مشابهة في الشرق الأوسط، لاستهداف الجمهور العربي بأخبار زائفة، وتقويض جهود الصحفيين في نقل الحقيقة، وإغراق منصات التواصل الاجتماعي بكمّ هائل من تلك الأخبار التي تستعرض قضايا تهم الناس. فمن ظاهرة ما يعرف بـ «الذباب الإلكتروني» ودوره في التأثير على «ترند» القضايا التي تشغل اهتمام جمهور منصات التواصل الاجتماعي والتلاعب بالنقاش الدائر حولها، إلى حملات استهداف النشطاء والصحفيين لتشويه سمعتهم، وصولا إلى حملات ممنهجة تسعى لترويج سردية واحدة تجاه القضايا التي تشغل الرأي العام، وإقصاء أي سردية أخرى.

إن الأخبار الزائفة وما تنطوي عليه من مخاطر تقوّض القيمة الجوهرية للصحافة -إخبار الناس بالحقائق-، وتساهم في زعزعة قدرة الجمهور على قراءة واقعه بمقاربة سليمة، وتدخله في حالة من الشك والحيرة أمام كل خبر وكل حدث يبرز في مجتمعه والعالم. في الوقت ذاته كانت هذه الشكوك كفيلة بأن تجعل مهمة الصحفي أكثر صعوبة في سعيه لإعادة الثقة بالإعلام، بعد أن استولت الأخبار الزائفة على منصات التواصل الاجتماعي، وأصبح تمييز الأخبار الحقيقية من غيرها، عملية مؤرقة وشاقة.

الخطر الأبرز الذي يحيق بالمجتمعات بسبب انتشار الأخبار الزائفة، هو بدء تلاشي ما يعرف بالفضاء العام (The Public Sphere) - وفق المفهوم الذي وضعه الفيلسوف الألماني يورغن هابرماس - والذي رأى كثير من الباحثين أنه تمثّل في مواقع التواصل الاجتماعي مطلع هذه الألفية، ولو بشكل جزئي؛ بعد أن خرج نقاش القضايا التي تهم العامة من احتكار صالونات النخب؛ إلى الساحات العامة (الافتراضية) التي أمّنتها منصات مثل فيسبوك وتويتر، في نقاش مفتوح دون قيود، كانت ثورات الربيع العربي أوج تجلياته. لكن انتشار الأخبار الزائفة والحملات المنظمة التي يقودها «الذباب الإلكتروني» ضد تلك النقاشات، أصبح يحول دون حدوثها في فضاء صحي. وبدل أن تسود القضية أو السردية التي تُجمع عليها الأغلبية في المجتمع وتتصدر الـ «ترند»، أصبح شخص واحد يسير آلاف الحسابات الوهمية قادرا على التأثير في تلك السردية؛ عبر توجيه تلك الحسابات لإقصاء أي «ترند» يقوده نشطاء مع أو ضد قضايا يرونها مهمة، ومنعه من الوصول لعامة الناس.

انطلاقا من هذه الحالة، وما تشكله من تهديد حقيقي لقيم الصحافة الجوهرية، دأب معهد الجزيرة للإعلام، خلال السنوات الماضية؛ على تقديم المعرفة لتوعية الصحفيين بمخاطر الأخبار الزائفة والتعريف بأفضل الممارسات لتجنب الوقوع في فخ تصديقها أو الترويج لها. بدأ المعهد مشروعه بإصدار «دليل التحقق من الأخبار»، ثم بترجمة كتاب «دليل التحقق للصحافة الاستقصائية» بالتعاون مع مركز الصحافة الأوروبي، وبإصدار كتاب «البحث عن الحقيقة في كومة الأخبار الكاذبة»، إضافة إلى نشر مقالات ودراسات تتناول الأخبار الزائفة عبر مجلة الصحافة وبرنامج زمالة الجزيرة. وفي سبيل إثراء المحتوى العربي، يأتي مشروع ترجمة هذا الكتاب إلى اللغة العربية، في مواجهة مستمرة بين الصحفيين من جهة، وبين الأخبار الزائفة وحملات التضليل الممنهجة من جهة أخرى.

معهد الجزيرة للإعلام

التحقق من عمليات التضليل والتلاعب الإعلامي

كريغ سيلفرمان

كريغ سيلفرمان هو محرر الوسائط الإعلامية في موقع BuzzFeed News، ومسؤول عن فريق عالمي لمتابعة المنصات، والمعلومات المضلِّلة، وحملات التضليل على وسائل الإعلام. سيلفرمان عمل على تحرير «دليل التحقق» و«دليل التحقق للصحافة الاستقصائية»، وهو مؤلف كتاب بعنوان:

«Lies, Damn Lies, and Viral Content: How News Websites Spread (and Debunk) Online Rumors, Unverified Claims and Misinformation»

في ديسمبر 2019، نشر المستخدم (@NickCiarelli)، مقطع فيديو يدّعي أنه لرقصة معروفة قام بأدائها مجموعة من الداعمين لمايكل بلومبيرغ في حملته الانتخابية لرئاسة الولايات المتحدة. هذا المقطع بما فيه من حماسة فاترة بين مَن ظهَر فيه من الناس وطريقةِ رقصهم لاقى انتشارًا واسعًا وتفاعَلَ معه الناس بشكل هائل بالإعجاب وإعادة التغريد، خاصة من المستخدمين الذين وجدوا في المقطع فرصة للسخرية من حملة بلومبيرغ وأنصاره. حصد المقطع بالمحصلة أكثر من 5 ملايين مشاهدة على تويتر.



Look out #TeamPete because us Bloomberg Heads have our own dance! Taken at the Mike Bloomberg rally in Beverly Hills. #Bloomberg2020 #MovesLikeBloomberg



12:10 AM · Dec 13, 2019 · Twitter for iPhone

2.7K Retweets 17K Likes

الوصف التعريفي بحساب المستخدم الذي نشر الفيديو يقول إنه متدرّب في حملة بلومبيرغ، وقد نشر تغريدات لاحقة ضمّنها لقطة من الشاشة يظهر فيها إيميل يدّعي أنه من أحد المسؤولين في حملة بلومبيرغ والذي أقرّ الميزانية الخاصة بمقطع الفيديو.

لكنْ، وعبْرَ عمليةِ بحث سريعة عن اسم المستخدم (Ciarelli) على جوجل تبين أنه اسم لكوميدي سبق أن أنتج فيديوهات مضحكة. أما الإيميل المنسوب إلى موظف حملة بلومبيرغ المزعوم، فلم يكن سوى رسالة أرسلها شريك هذا الكوميدي، واسمه براد إيفانز، وهي معلومة ساعد جوجل في الحصول عليها أيضًا بكل سهولة.

لكن يبدو أن البعض صدّق فعلا -على مدار الدقائق والساعات الأولى مِن نشْر الفيديو- أنّ هذا المقطع المثير للسخرية هو فعلًا إنتاج رسمي من قبل حملة بلومبيرغ.

ماغي هابرمان (Maggie Haberman)، وهي مراسلة معروفة في القسم السياسي في نيويورك تايمز غردت على حسابها في تويتر بأن الصحفيين الذين تابعوا الحملات السابقة لمايكل بلومبيرغ كان لديهم مسوّغ لعدم الشكّ في موثوقية الفيديو:



The guys who created the Bloomberg parody video can't understand why reporters who covered Bloomberg previous campaigns didn't instantly recognize it as parody >



The True Story Behind the Viral 'Moves Like Bloomberg' Video
vulture.com

للمعرفة أشكال عديدة، وحريّ بالصحفيين والصحفيات في هذه البيئة الرقمية الجديدة أن يكونوا حذرين من الاعتماد بشكل مفرط على أي مصدر واحد من المعلومات، حتى لو كانت تجربة شخصيّة خاصة بهم.

ويبدو أن بعض الصحفيين الذين أَلِفوا طابع بلومبيرغ وأسلوب حملاته الانتخابية، شعروا أن الفيديو لا يُستبعد أن يكون قد صدر عن حملته فعلا. لكن في الوقت ذاته، كان يمكن للصحفيين غير المطلعين عن كثب على حملة بلومبيرغ أن يتوصلوا للجواب الصحيح لو اختاروا الحكم على الفيديو عبر التدقيق في مصدره، ولم يكن ذلك يحتاج سوى البحث في جوجل عن اسم صاحب الحساب الذي شارك المقطع.

لسنا نفترض هنا أن ثمة تجربة سلبية بالضرورة في تغطية حملات بلومبيرغ، لكن الفكرة هي أننا يمكن أن نتعرض للتضليل في أية لحظة عبر ما نفترض أننا على دراية به. وفي بعض الحالات، قد تكون الأسس التي قامت عليها معرفتنا وتجاربنا بخصوص شخص أو أمر ما غير سليمة. كما يمكن أيضًا أن نقع ضحية بعض المؤشرات الرقميّة مثل حجم الزخم الذي يحظى به مقطع الفيديو من أعداد المشاهدات وإعادات التغريد، أو عبر المساعي التي تُبذَل للتلاعب بها.

يتبين لنا عبر هذا المثال أنه يمكن وبخطوات بسيطة خلق مؤشرات مضللة؛ مثل وضع تعريف شخصي مختصر (Bio) على تويتر، أو لقطة شاشة (Screenshot) من رسالة بريد إلكتروني قد تدعم محتوى أو ادعاءً ما، وهي عناصر تساعد على انتشارها السريع. وكلما حازت تغريدة ما على المزيد من الإعجابات وإعادات التغريد، فإنها ستُضحي أكثر إغراءً للآخرين للتصديق بأن محتواها حقيقيّ.

لا شكّ أنه يتوفر العديد من الأمثلة التي تفوق هذا المثال خبثًا. وبخلاف سياريلي في المثال السابق، فإن الأشخاص النشطين في العمليات الخاصة بالترويج وحملات المعلومات المضللة لا يكشفون عن الحيلة بسهولة. لكن الحالة التي استعرضناها أظهرت مقدار الإرباك والإحباط الذي قد يواجهه أي شخص -بما في ذلك الصحفيون- أثناء محاولة تلمُّس الحقيقة في بيئة من المعلومات التي تعجّ بالمؤشّرات التي يسهل التحكّم بها، لتُضفي المزيدَ من الجودة والموثوقية على ما يجري ترويجُه.

الثقةُ هي إحدى اللَّبِنات التي يقوم عليها المجتمع، وهي العملة التي تساعد في تسهيل مختلف أشكال التعاملات، وهي أيضا عنصر أساسي في التواصل والعلاقات. ورغم ذلك، فإنه من الخطورة بمكان افتراض الثقة أثناء التعامل مع البيئة الرقمية التي نعيش ضمنها.

فإن كنت تنطلق من افتراض الثقة بأن حسابات تويتر التي تعمل على إعادة تغريد مقطع فيديو ما جميعها تقوم بذلك بشكل عفوي، فلا شكّ أنك ستقع ضحية للتلاعب. ولو كنت تثق فورًا بالتقييمات الموضوعة على منتج ما وتفترض أنها جميعها من عملاء حقيقيين، فلا شكّ أنك ستخسر نقودك. ولو كنت تثق بأن كل مقال تطّلع عليه يمثّل عرضًا محايدًا تمامًا لما يلزمك معرفته من معلومات عن قضيّة ما، فستكون عرضة لاستهلاك معلومات مضللة.

من الضروري للجميع -ولا سيّما الصحفيين- التنبّه لهذه القضية. فنحن حاليًا مستهدفون بحملات منسّقة وممولة بشكل سخيّ للاستحواذ على انتباهنا، وتمرير رسائل وأجندات معينة، وتطويعنا جميعًا لصالح الحكومات أو غيرها من القوى الفاعلة.

لكن الجانب الإيجابي هنا هو أن هذا الواقع يخلق فرصة، وواجبًا، لامتلاك القدرة على التحقّق والشكّ.

هذا الدليل هو خلاصة معارف وخبرات لعدد من الصحفيين والباحثين الذين يطمحون إلى تقديم إرشادات تتعلق بكيفية تنفيذ عمليات التحقق في مواجهة حملات التلاعب والتضليل والترويج في الوسائط الرقمية.

نحن ننشط في منظومة معلوماتية بالغة التعقيد وسريعة التغيّر، ولا بدّ أن يكون في إزائها منهجية تُكافئها في القدرة على التطوّر والتكيّف، تكون قائمة على الشكّ الأولي في افتراضاتنا، وقادرة على تعقب وتوقع أنماط سلوك الطرف المقابل، بالاستفادة من أفضل الأساليب المتاحة في التحقق وإعداد التقارير اعتمادا على المصادر المفتوحة.

إن نقـاط الهشاشـة فـي عالمنـا الرقمـي المرتبـط بالبيانـات تتطلـب مـن الصحفييـن أن يُعملـوا مبضـعَ الشـكّ والتمحيـص فـي كل مـا يَعْـرِض لهـم فـي هـذا العالـم، وأن يسـتفيدوا مـن مهاراتهـم مـن أجـل توجيـه العامـة نحـو المعلومـات الدقيقـة التـي يمكـن الثقـة بهـا. هـذه البيئـة تتطلـب مـن الصحفييـن أيضًـا أن ينظـروا فـي احتمـال أن نسـاهم نحـن -وعـن غيـر قصـد- فـي منـح فرصـة لبـروز أصـوات غيـر نزيهـة أو حمـلات مصمَّمـة لاسـتغلالنا، والتسـرّع فـي توجيـه أصابـع الاتهـام إلـى أطـراف فاعلـة فـي الدولـة مثـلًا؛ حين تكون "الأدلة" ضدّها.

إن الهـدف مـن هـذا الدليـل هـو تزويـد الصحفييـن بالمهـارات والأسـاليب التـي تلزمهـم فـي أداء عملهـم بفعاليـة ومسـؤولية. كمـا يقـدم الدليـل أرضيـة أساسـية فيمـا يخـص النظريـة والسـياق والجاهزيـة الذهنيـة بمـا يمكّـن الصحفييـن مـن القيـام بأعمـال عاليـة الجـودة تقـدِّم المعلومـات الدقيقـة للعامـة، وتَفضـح الفاعلين السلبيين في بيئة الإعلام والمعلومات وتعمل على تحسينها.

لكـنْ أولُ مـا يجـب التأكيـد عليـه هـو أن المعرفـة العمليـة والأدوات المتوفـرة لـن تجـدي نفعًـا إلا عنـد مقاربـة هـذا العمـل مـن عقليـة واعيـة. المقصـود هنـا هـو أن يقتنـع الصحفـي أو الصحفيـة بـأن أي شـيء فـي البيئـة الرقميـة قابـل لأن يكـون مـادة للتلاعـب والتضليـل، وأن يـدرك أن ثمـة نطاقًـا واسـعًا مـن الأفراد والهيئات التي لديها الدافع للقيام بذلك.

مـا يميّـز البيئـة الرقميـة هـو أنـه فـي كثيـر مـن الأحيـان ثمـة أثـر مـن بيانـات مـا، أو أشـكال تفاعـل أو صـلات أو غيرهـا مـن العلائـق الرقميـة التـي يمكـن تتبعهـا، وكثيـر منهـا قـد يكـون متوفـرًا وفـي متنـاول اليـد بشـرط أن يعـرف المرء كيف وأين يبحث.

إن التحقـق فـي البيئـة الرقميـة يعنـي عـدم التعاطـي مـع أي شـيء بحسـب مـا يظهـر لنـا، كمـا يعنـي أنْ نـدرك أنّ بعـض العناصـر التـي قـد تظهـر لنـا قابلـة للإحصـاء ومرتبطـة بالبيانـات، مثـل عـدد الإعجابـات والمشـاركات وإعـادات التغريـد والزيـارات (الترافيـك) ومراجعـات المنتجـات والنقـرات علـى

الإعلانـات، هـي أيضًـا عناصـر يمكـن التلاعـب فيهـا بسـهولة، بـل هـو فـي الواقـع مـا يحصـل فـي كثيـر مـن الحـالات. إن التحقـق يعنـي إدراك أن الصحفييـن هـدف أساسـي لحمـلات التلاعـب الإعلاميـة والترويـج المعلوماتي، بمعنـى أن هـذه الحمـلات موجّهـة لهـم أو ضدّهـم، كمـا أنهـم القنـاة الأساسـية التـي يتـم عبرهـا نشـر المعلومـات الخاطئـة أو المضللـة. إنـه يعنـي أن تتسـلح أنـت وزمـلاؤك بالتوجـه أو بالعقـل الواعـي، والأسـاليب والأدوات الضروريـة لضمـان أداء دورك فـي تقديـم المعلومـات الموثوقـة والدقيقـة، وعـدم تضخيـم الأكاذيب والمحتوى المضلِّل أو حملات التصيّد.

هـذا التوجّـه الواعـي يرتبـط بمعادلـة واضحـة: عبـر تعطيـل الثقـة التلقائيـة بـكل مـا نتعـرض لـه، سـيكون بوسـعنا الانخـراط فـي عمـل مـن شـأنه أن يكشـف عمّـا هـو موثـوق مـن سـواه. وهـذا هـو فـي المقابـل سـبيلنا مـن أجـل إنتاج عمل صحفي يمكن للمجتمعات التي نخدمها أن تثق به.

إلـى جانـب هـذا، ثمـة بعـض الأساسـيات التـي سـتتكرر فـي الفصـول ودراسات الحالة التي سنتعرض لها:

- **فكّر بعقليّـة الخصم.** كل سـمة جديـدة فـي منصـة أو خدمـة رقميـة مـا قـد تكـون عرضـة للاسـتغلال بطريقـة أو بأخـرى. ومـن الضـرورة بمكان أن تضـع نفسـك فـي مـكان الشـخص الـذي يحـاول أن يتلاعـب بهـذه البيئـة الرقميـة لأغـراض أيديولوجيـة أو سياسـية أو ماليـة أو سـواها. فحيـن تنظـر إلـى المحتـوى والرسـائل الرقميـة، عليـك أن تفكـر فـي الدوافـع التـي أدت إلـى إنشـائها وترويجهـا فـي المقـام الأول. ولا يمكـن أيضًـا الاسـتغناء عـن الاطـلاع علـى أحـدث التقنيـات التـي تسـتخدمها الأطـراف ذات الدوافـع السـلبية، سـواء الأطـراف التـي تنشـئ المحتـوى أو تسـوّق لـه رقميًـا وغيرهـا مـن الأطـراف التـي تعتـاش علـى إيجـاد سـبل جديـدة لجذب الاهتمام أو توليد الأرباح في البيئة الرقمية.

- **ركـز علـى الأطـراف الفاعلـة، والمحتـوى، والسـلوك، والشـبكات.** يتمثـل الهـدف فـي تحليـل الأطـراف الفاعلـة، والمحتـوى، والسـلوك،

وتوثيق كيف يمكن أن تعمل جميعها في شبكة واحدة. وعبر مقارنة ومقابلة هذه العناصر الأربعة فيما بينها، سيكون بوسعك أن تفهم ما تراه بجلاء. وكما سترى في الفصول ودراسات الحالة في هذا الكتاب، فإن إحدى المنهجيات الأساسية في العمل تكمن في البدء بطرف من البيانات أو من موقع إلكتروني والبناء على ذلك؛ سعيًا إلى تحديد شبكة أكبر، عبر تحليل نمط السلوك وغير ذلك من الروابط. وقد يشمل ذلك تحليلَ طبيعة تدفق المحتوى، والأطراف الفاعلة عبر المنصات، إضافة إلى تتبع المحتوى بلغات أخرى.

• **المراقبة والجمع.** إن أهم طريقة في اكتشاف التلاعب الإعلامي والمعلومات المضللة هي مداومة البحث عنها في جميع الأوقات. ولا بدّ من استمرار المراقبة والتعقب للفاعلين والمواضيع محل الاهتمام، والمجتمعات المعنية. لذلك احتفظ ونسّق ما تتمكن من العثور عليه، سواء في جداول، أم في ملفات تشتمل على صور مقتطعة من الشاشة (Screenshots)، أو عبر استخدام أدوات مدفوعة مثل Hunchly.

• **حذارِ من التسرّع.** قد يكون من المستحيل أحيانًا الجزم بشكل قاطع بشأن هويّة من يقف وراء إنشاء حساب أو محتوى أو حملة ما. أحد أسباب ذلك هو أن بعض الأطراف -رغم اختلاف دوافعها- قد تتصرف بطرائق متشابهة، فتُنتج أو تروّج لمحتوى من نوع واحد.

بل إنّ المنصات نفسها -رغم ما يتوفر لديها من مصادر وقدرة أفضل إلى الوصول إلى البيانات- قد تخطئ أحيانًا في تحديد مرجعيّة المحتوى وأصله.

وعادة ما تكون الأدلة الأكثر نجاحًا وإقناعًا هي تلك الأدلة التي تجمع بين الدليل الرقمي مع المعلومات التي يتم تحصيلها من مصادر داخلية، وهذه هي التركيبة المثالية بين العمل الاستقصائي التقليدي والرقمي.

ولا شكّ أن التوصل إلى مثل هذه الأدلة قد بات أكثر صعوبة، ولاسيما مع التطوّر في أداء الأطراف في السلطة أو في سواها، واعتمادهم على طرائق جديدة لإزالة أي أثر يدلّ على تورّطهم. نسبة نشاط رقمي ما إلى طرف أصلي محدد أمر بالغ الصعوبة، وأي خطأ في ذلك من شأنه أن يقوّض كل الجهود الدقيقة التي قادتنا إليه في المقام الأول.

أودّ أخيرًا أن أشير إلى أن هذا الدليل هو ثمرة جديدة للجهود التي بُذلت في النسخة الأولى من دليل التحقق، إضافة إلى دليل التحقق للصحافة الاستقصائية. وكلٌّ واحد من هذه الأدلة يشتمل على مهارات أساسية تساعد في مراقبة المحتوى في وسائل التواصل الاجتماعي، والتحقق من الصور ومقاطع الفيديو، وحسابات مواقع التواصل الاجتماعي، واستخدام محركات البحث في تحديد الأفراد والشركات وغيرها من الكيانات.

وبناء على ذلك فإن العديد من الفصول ودراسات الحالة الواردة في هذا الدليل قد كتبت على افتراض أن القراء محيطون بالمعلومات والإرشادات والأدوات التي وردت في الدليلين السابقين، وخاصة الدليل الأول. وفي حال وجد القارئ صعوبة في التعاطي مع المعلومات في هذا الدليل، فإنه يُنصح بالبدء من الأساسيات والاطلاع على الدليل الأول. أمّا الآن، فهيّا إلى العمل!

عصر فوضى المعلومات

كلير واردل

كلير واردل هي مديرة التوجيه الإستراتيجي والأبحاث في مؤسسة "فيرست درافت" (First Draft)، وهي مؤسسة عالمية غير ربحية لدعم الصحفيين والأكاديميين والتقنيين الذين يسعون إلى التعامل مع التحديات المتعلقة بمسائل الموثوقية والحقيقة في العصر الرقمي. حازت كلير واردل على زمالة مركز شورنستين للإعلام والسياسة والسياسات العامة في كلية كينيدي بجامعة هارفرد، وشغلت منصب مديرة الأبحاث في مركز تاو للصحافة الرقمية في كلية الصحافة بجامعة كولمبيا، إضافة إلى مديرة شؤون وسائل التواصل الاجتماعي في المفوضية العليا للأمم المتحدة لشؤون اللاجئين.

نعلم جميعنا أن الشائعات والبروباغندا ليست مفاهيم أو ظواهر طارئة، فالإنسان منذ القدم امتلك هذه القدرة على اتباع أنماط سلوك تشتمل على الخداع والتضليل، وثمة الكثير من القصص التي خلدها التاريخ والتي تتحدث عن استخدام المعلومات الزائفة من أجل تضليل العامة أو محاولة الإطاحة بحكومة ما أو رفع أسعار الأسهم في أسواق التداول.

لكن الفرق اليوم هو مدى سهولة القيام بأنشطة مشابهة، حيث يعمد أيٌّ شخص إلى خلق محتوى مزيف ومضلل، إضافة إلى سرعة انتشار هذا المحتوى ونطاق تأثيره العالمي.

لطالما فهمنا أن ثمة تعقيدًا في مسألة الخداع والتضليل، فليس لدينا وصفة واحدة تنطبق على الجميع. فكذبة "بيضاء" تخرج عن شخص يسعى

للمصالحة بين أفراد العائلة ليست مثل بيان مضلل يصدر عن سياسي بهدف كسب المزيد من الأصوات. كما أن حملة بروباغندا تقودها الدولة ليست بالتأكيد مثل نشر أفكار غارقة في نظرية المؤامرة عن رحلة الهبوط على القمر.

ومن المؤسف أن ما حصل في الأعوام القليلة الماضية هو استسهال وضع جميع الأمثلة التي وردت أعلاه في خانة واحدة: "أخبار زائفة"، وهو مصطلح بسيط شاع في العالم أجمع وصار يتردّد على ألسنة الجميع، حتى بلفظه الإنجليزي "Fake News"، دون حاجة إلى الترجمة.

وهذا مؤسف في نظري لأن المصطلح غير كاف لبيان مستوى التعقيد الحاصل. فالنسبة الغالبة من المحتوى الخادع لا يُقدَّم أصلًا على أنه أخبار. فنحن نتعامل هنا مع "الميمات" (Memes)، ومقاطع فيديو، وصور، أو أنشطة منسقة على تويتر أو يوتيوب أو فيسبوك أو إنستغرام. وغالبية ما ينشر ليس زائفا، بل مضلِّل، أو، وكما في أغلب الأحيان، محتوى أصلي لكن يُنزع من سياقه.

ومن المعلوم أن المعلومات المضللة الأكثر تأثيرًا هي تلك التي تشتمل على طرف خيط من الحقيقة: فتأخذه وتسيء استخدامه ووصفه، أو تعيد نشره للإيهام بأنه جديد رغم أنه انقضى عليه عدة سنوات.

الأمر الأكثر إشكالًا ربما هو أن مصطلح الأخبار المزيفة قد صار "التهمة" الجاهزة التي يتلقفها السياسيون وأنصارهم لمهاجمة وسائل الإعلام المهنية حول العالم.

انزعاجي من هذا المصطلح دفعني إلى سبك مصطلح آخر، هو "فوضى المعلومات"، وقد توصلت إليه مع زميلي حسين درخشان. فقد تعاونّا معًا عام 2017 في كتابة تقرير بعنوان "فوضى المعلومات"، وتحدثنا عن الإشكالات المصطلحية حول هذا الموضوع. في هذا الفصل،

سأوضح عددًا من الجوانب الأساسية في التعريف من أجل الإحاطة بالموضوع، ومقاربته بشكل نقدي.

7 أشكال من فوضى المعلومات

وضعت في العام 2017 هذا التصنيف من أجل بيان الأشكال المختلفة لفوضى المعلومات.



السخرية أو التهكم

وجدتُ معارضةً من بعض الزملاء الباحثين حين ناقشتهم في مسألة السخرية والتهكم ووضعها في هذا التصنيف الخاص بفوضى المعلومات، وأنا أتفهم تمامًا وجهة النظر التي انطلقوا منها في معارضة ذلك، ولاسيما أنني شخصيًا ترددت كثيرًا قبل أن أُدرجها في التصنيف.

لكن الحاصل -مع الأسف- هو أن العديد ممن يولِّدون وينشرون المعلومات المضللة يقومون بشكل مقصود بإضفاء سمة التهكم أو السخرية من أجل

ضمان ألّا يخضع محتواهم لضوابط "التحقق من المحتوى"، وكوسيلة استباقية للتنصل من أي ضرر قد ينجم عن نشر هذا المحتوى.

ففي منظومة المعلومات، حين يتم حذف السياق أو الدلائل، أو الاستدلالات الذهنية (Mental Heuristics)، فإن المحتوى الساخر سيكون كفيلًا عادة بالتسبب بالإرباك لدى القارئ. قد يعرف الأمريكي مثلًا أن موقع "The Onion" هو موقع للأخبار الساخرة، لكن لعلك لا تعلم أن ثمة أكثر من 57 موقعًا للأخبار الساخرة عالميًا. فإن لم تكن تعلم أن الموقع يقدم أخبارًا ساخرة، ومر عليك منشور لهذا الموقع أثناء تصفحك فيسبوك مثلًا، فيمكن بسهولة أن تُخدع وتصدِّق ما قرأته.

اتخذت منصة فيسبوك مؤخرًا قرارًا بعدم التحقق من المحتوى الساخر، لكن العاملين في هذا المجال يعرفون تمامًا كيف أن وسم محتوى ما بالساخر ليس إلا حيلة مقصودة من قِبل صناع هذا الشكل من المحتوى.

في أغسطس 2019، نشر موقع Snopes مقالًا عن السبب الذي يدفع المحررين في الموقع للتحقق من المقالات في المواقع الساخرة. إن ما ينشر تحت مسمّى "محتوى ساخر" هو وسيلة لتجنّب الوقوع تحت تمحيص مواقع وأدوات التحقق من الأخبار، لكن ما يحصل في واقع الأمر هو أن المحتوى الأصلي يضيع، ويستمر الناس في مشاركة وإعادة نشر المحتوى الساخر، دون إدراك أنه ساخر، ليحلّ في المحصّلة مكان ما هو حقيقيّ.

الربط الكاذب

هذا طُعم قديم ومعروف: وهو عرض ادعاءات بخصوص المحتوى؛ عبر استخدام عنوان مثير؛ لدفعك إلى النقر وتصفح ذلك الخبر، لتكتشف أن ذاك العنوان لا علاقة له بتاتًا بالمقال أو بالمحتوى المنشور.

وبالرغم من أنه قد يسهّل على وسائل الإعلام التعاطي مع مشكلة المعلومات المضلِّلة على أنها مجرد معلومات تُقدَّم من قِبل فاعلين سلبيين، إلا أنني أرى أنه من الضروري الاعتراف بأن بعض الممارسات غير المهنية ضمن حرفة الصحافة تزيد هي الأخرى من التحديات المتعلقة بفوضى المعلومات.

محتوى مضلل

لطالما شكّل المحتوى المضلّل معضلة في ميدان العمل الصحفي وفي عالم السياسة. سواء كان ما يحصل اقتطاع اقتباس مجزوء ووضعه خارج سياقه، أم اختلاق إحصاءات تدعم ادعاءً ما؛ دون الأخذ بالاعتبار الطريقة التي جمعت بها البيانات، أم قصّ صورة لتأطير القصّة وفق طريقة معينة مخالفة لما تدل عليه الصورة الأصلية. كل هذه الممارسات المضلِّلة ليست بالأمر الجديد بطبيعة الحال.

السياق المغلوط

هذه هي الفئة التي نرى فيها النسبة الأكبر من محتوى فوضى المعلومات: وهو ما يحدث كثيرًا عند إعادة استخدام صور حقيقية لكنها قديمة، ونشرها على أنها جديدة. يحصل ذلك عادة مع الأخبار العاجلة، فتطفو على السطح صور قديمة ويعاد نشرها بشكل كبير. كما يحدث ذلك عند إعادة نشر مقالات أخبار قديمة وكأنها جديدة، خاصة حين يكون العنوان متقاطعًا مع أحداث راهنة.

المحتوى الكاذب

يحصل ذلك مثلًا عند استخدام شعار مؤسسة معروفة أو اسم شخص

معيّن، مع محتوى ليس من إنتاجه. ولهذه الوسيلة فعالية خاصة؛ لأنها تلعب على إمكانات الاستدلال المرتبطة بهذه الصور. وعادة فإن إحدى أفضل الطرق التي نستخدمها في الحكم على المحتوى هي النظر إلى مقدار ثقتنا بالمؤسسة أو الشخص الذي يقدمه. لذا فإن استغلال شعار مؤسسة إخبارية موثوقة وإضافتها إلى صورة أو مقطع فيديو، سيزيد من فرصة ثقة الناس بهذا المحتوى دون التحقق منه.

محتوى متلاعَب به

يحصل ذلك حين يتم التلاعب والعبث بمحتوى أصلي بطريقة معينة لأغراض التضليل. ومن أمثلة ذلك فيديو نانسي بيلوسي في مايو 2019. تم تصوير رئيسة مجلس النواب الأمريكي نانسي بيلوسي وهي تلقي خطابًا. بعد ساعات من ذلك، انتشر مقطع فيديو تظهر فيه بيلوسي تتحدث كما لو أنها ثملة. لقد تم التلاعب بالفيديو عبر تبطيء سرعته، فبدت بيلوسي ثقيلة اللسان. وهذا أسلوب مؤثر وفعال، لأنه يعتمد على محتوى أصلي. ولأن الناس يعرفون أن بيلوسي ألقت بالفعل خطابًا، فإن هذا قد يدفعهم إلى تصديق المقطع الذي تم التلاعب به.

محتوى مُفبرك

وهذه الفئة تعني المحتوى المزيف بشكل كامل، مثل قيام شخص بإنشاء حسابات باسم وهمي على وسائل التواصل الاجتماعي ويبدأ بنشر محتوى جديد عبرها. وتشمل هذه الفئة أيضًا عمليات "التزييف العميقة" (Deep-fakes)، والتي تعتمد على الذكاء الاصطناعي في تصنيع مقاطع فيديو أو صوت ليظهر فيها شخص ما ويحاك على لسانه (حرفيًّا) كلامٌ لم يصدر عنه إطلاقًا.

فهم القصد والدافع

يساعدنا هذا التقسيم على توضيح مستوى التعقيد في بيئة معلومات "ملوّثة"، لكنه لا يتناول جانب "القصد"، وهو عنصر بالغ الأهمية في فهم هذه الظاهرة.

لذلك قمت أنا ودرخشان بإنشاء هذا المخطط البياني من أجل توضيح الفرق بين المعلومات المغلوطة (Misinformation)، والمعلومات المضلِّلة (Disinformation)، والمعلومات الخبيثة (Malinforma-tion). المعلومات المغلوطة والمضللة والخبيثة أمثلةٌ على المحتوى المزيف، لكن الفرق هو أن:

المعلومات المضللة تكون من صنيعة وترويج جهات تهدف إلى خلق الضرر، سواء كان ماليًا أم سياسيًا أم ماديًا أم يتعلق بسمعة شخص أو جماعة ما.

أما **المعلومات المغلوطة**، فهي معلومات ليست صحيحة، ولكن الناس الذين ينشرونها لا يدركون ذلك. وهذا ما يحدث عادة في لحظات الأخبار العاجلة، حين يبدأ الناس بمشاركة شائعات أو صور قديمة دون أن يدركوا أنها ليست مرتبطة بالأحداث الجارية.

أما **المعلومات الخبيثة** (Malinformation)، فهي معلومات صحيحة، لكن الجهات التي تبدأ بنشرها تهدف إلى التسبب بالضرر. فتسريب رسائل البريد الإلكتروني الخاصة بهيلاري كلينتون خلال الحملة الانتخابية الأمريكية عام 2016 هو مثال على ذلك، ويدخل في ذلك أيضًا مشاركة صور أو مقاطع فيديو إباحية على سبيل الانتقام.

أشكال فوضى المعلومات

قصد الضرر

عدم الصحّة

المعلومات الخبيثة

النشر المقصود لمعلومات خاصّة: لدوافع شخصية أو لخدمة أغراض شركة أو جهة ما، وليس للصالح العام، مثل "الإباحية الكيدية"، أو التغيير المقصود للسياق أو التاريخ أو الزمن الخاص بمحتوى صحيح.

المعلومات المضللة

محتوى مزيف أو متلاعب به بشكل مقصود سواء كان محتوى صوتيًا أم مرئيًا، إضافة إلى نظريات المؤامرة والشائعات التي يتم اختلاقها بشكل مقصود.

المعلومات المغلوطة

أخطاء عفوية في نشر المعلومات، مثل وصف غير دقيق للصور، أو خطأ في التاريخ، أو الأرقام، أو الترجمة، أو حين يتم التعامل مع المحتوى التهكمي الساخر على أنه حقيقي.

هذه المصطلحات مهمّة، وذلك لأن تحديد القصد وراء أي سلوك يساعد على تحديد كيفية فهمه. هنالك **ثلاثة دوافع** أساسية لوضع محتوى مغلوط أو مضلل.

الأول هو **الدافع السياسي**، سواء كان ذلك في السياسة الداخلية أم في الخارجية. فقد يكون ذلك محاولة من طرف حكومة أجنبية للتأثير في مسار الانتخابات في بلد آخر. كما يمكن أن يحصل ذلك محليًا، حيث تلجأ حملة لطرف سياسي ما إلى أساليب "قذرة" من أجل تشويه سمعة الخصم.

الدافع الثاني هو **الدافع المالي**. فمن الوارد مثلًا جنيُ المال عبر جذب الإعلانات على موقعك الإلكتروني. فإنْ كنت تلجأ إلى نشر مقالات مغلوطة في مواضيع حساسة بعناوين ضخمة ومثيرة تغري الناس على النقر على الرابط، فإن هذا يعني المزيد من المال.

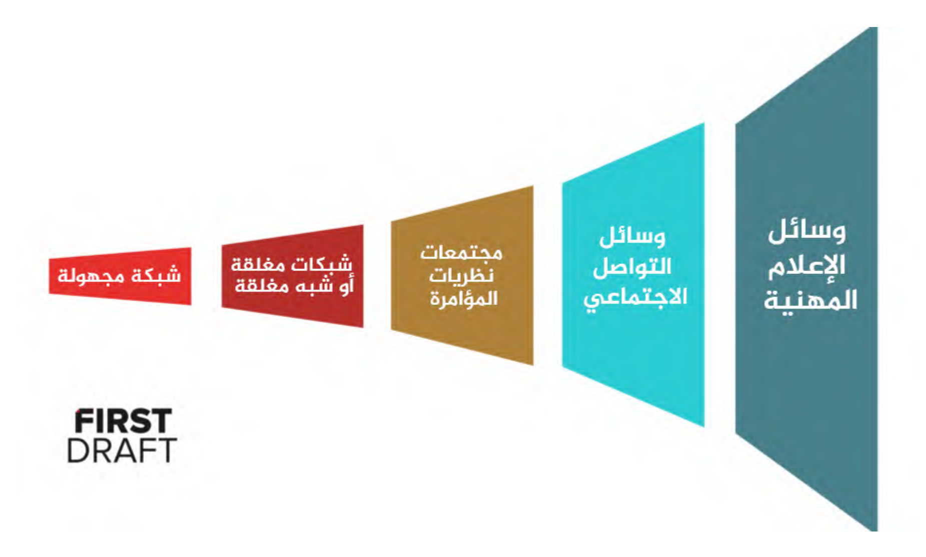
وثمة العديد من الناس من مختلف التوجهات السياسية تحدثوا عن كيفية إنشاء مواقع "أخبار" مزيفة، لمجرد الرغبة في جذب المزيد من الزوار وجني المال.

وهنالك أخيرًا **الدوافع الاجتماعية والنفسية**. فالبعض ببساطة يكون مدفوعًا بالرغبة لإثارة الجدل والفضول بمعرفة ما قد يترتّب على فعلته، كأن يرى إن كان قادرًا على خداع الصحفيين، أو دفع الناس للتوجّه إلى مكان ما للتظاهر من خلال دعوة عبر فيسبوك، أو إشباع رغبته في التنمر أو التحرش بالنساء. وهنالك كثيرون يلجؤون إلى نشر المعلومات المغلوطة، لمجرد الرغبة بتقديم صورة ما عن أنفسهم. فقد يقول أحدهم مثلًا: لا أكترث إن كان هذا صحيحًا أو لا، كل ما أريده هو أن أثبت لأصدقائي على فيسبوك مقدار بغضي لهذا المرشّح".

أبواق التضخيم

من أجل فهم دقيق لهذه المنظومة بنطاقها الأوسع، علينا أن ننظر إلى مقدار التشابك الحاصل. كثيرًا ما يقع نظر شخص على محتوى مضلل أو مغلوط في مكان ما، ويعتقد أن هذا المكان هو المصدر الأصلي لهذا المحتوى. ولسوء الحظ فإن الأطراف الأكثر تأثيرًا في بث المعلومات المضللة هم أولئك الذين ينجحون في استغلال هذه الطبيعة المتشظّية للمحتوى.

حريّ بنا أيضًا التذكر أنه لو لم يجرِ نشر ومشاركة للشائعات أو نظريات المؤامرة أو المحتوى غير الصحيح، فإنه لن يترتب عليها أي ضرر. لأن الضرر يكمن في عملية مشاركة وترويج ذلك المحتوى. لذلك أنشأتُ هذا الرسم البياني لبيان فكرة "أبواق التضخيم"، كي أوضّح طريقة توظيف الأطراف التي تقف وراء المعلومات المضللة لعمليات منسقة من أجل بثّ الحياة في هذا النوع من المعلومات في هذه المنظومة.



كثيرًا ما يتم نشر محتوى في مساحات مثل "فورتشان [1] 4Chan" أو ديسكورد [2] Discord، وهي مساحات يتم فيها وضع منشورات مؤقتة بهوية مجهولة، وعادة ما يتم الاستفادة منها من أجل مشاركة تفاصيل معينة بهدف التنسيق، مثل أن يدعو أحدهم إلى استخدام هاشتاغ وتصعيده، أو استخدام "ميم" معين للتفاعل مع قضية ما على فيسبوك.

بعدها ينتقل هذا التنسيق إلى مجموعات رسائل مباشرة كبيرة على تويتر، أو واتساب، حيث يجري نشر محتوى من قبل أطراف معينة في الشبكة لتصل إلى مجموعة أكبر من الأشخاص. ثم قد ينتقل المحتوى إلى مجتمعات على مواقع إلكترونية مثل "غاب" (Gab)، أو ريديت (Reddit)، أو يوتيوب. ومن هنالك يبدأ المحتوى عادة بالظهور بشكل أوسع على منصات مثل فيسبوك أو إنستغرام أو تويتر.

ثم تلتقط وسائل الإعلام المهنية هذا المحتوى الذي صار رائجًا، إما لأن الصحفي لم يستطع تحديد أصل هذا المحتوى ويقرر أن يستفيد منه في تقرير ما، دون اللجوء إلى ما يلزم من عمليات التحقق الكافية، وإمّا لأنه يقرر أن يفنّد هذا المحتوى بالأدوات المتوفرة لديه. وعلى كلا الحالين

[1] منصة لنشر الصور بشكل مجهول دون معرفة هوية من ينشر تلك الصور.

[2] تطبيق يستخدم للتواصل بين محترفي الألعاب الإلكترونية.

فـإن ذلـك يعتبـر نجاحًـا للأطـراف التـي أنشـأت هـذا المحتـوى المضلـل. فالعناويـن ذات الصياغـة الإشـكالية التـي تشـير إلـى إشـاعة أو خبـر مضلـل، أو حتـى المحتـوى المضـادّ الـذي يسـعى إلـى تفنيـد الخبـر المضلـل، يسـهم فـي إنجاح المقصد الأساسي، وهو تضخيم الخبر وخلق حيّز أوسع لانتشاره.

كثيـرًا مـا نتطـرق فـي "فيرسـت درافـت" إلـى فكـرة "النقطـة الحرجـة" التـي تسـتدعي التدخّـل الصحفـي عنـد بلوغهـا. فاسـتعجال الصحفييـن فـي الحديـث عـن أخبـار مضللـة بشـكل مبكّـر جـدًا قـد يكـون بمثابـة سـكب الزيـت علـى نـارٍ شـائعةٍ بالـكاد اشـتعلت. كمـا أن التأخـر فـي دحضهـا يعنـي أنها قـد وصلت حـدًّا يصعـب معـه إزالـة الضـرر الحاصـل. لـذا فـإن تقديـر هـذه "النقطـة الحرجـة" يضحـي أمـرًا مهمًـا رغـم صعوبتـه وتعقيـده، لأن ذلـك يختلـف باختلاف المكان والموضوع والمنصّة.

خاتمة

عنـد الحديـث عـن ظاهـرة بهـذا الحجـم مـن التعقيـد، فـإن الكلمـات التـي نوظفهـا يكـون لهـا تأثيـر كبيـر فـي طريقـة التعاطـي معهـا. لدينـا العديـد مـن الأبحـاث الأكاديميـة التـي تُظهـر توجهًـا متزايـدًا بيـن العامـة للخلـط بيـن "الأخبـار الزائفـة" وبعـض مظاهـر الخلـل المهنـي التـي تطـرأ فـي وسـائل الإعلام المهنية.

إن التسـاهل فـي إطـلاق وصـف "معلومـات مضللـة" علـى أشـكال مختلفـة مـن المحتـوى، يعنـي فقـدان القـدرة علـى التمييـز بيـن مـا هـو مفبـرك فعـلًا أو صحيـح ويجـري تداولـه بين النـاس تحـت وصـفٍ خاطـئ أو فـي سـياق غيـر صحيـح، مـا يعنـي بالمحصلـة عـدم القـدرة علـى الإحاطـة بحقيقـة مـا يحصـل ودوافعه وأبعاده.

نحـن نعيـش فـي عصـر فوضـى المعلومـات، وهـو واقـع يخلـق العديـد مـن التحديـات الجديـدة للصحفييـن والباحثيـن والمختصيـن فـي مجـال المعلومـات

والمحتوى. هل أتناول كصحفي محتوى رائجًا ما؟ ومتى أفعل ذلك؟ كيف أصوغ العنوان المتعلق بهذا المحتوى؟ وكيف أكشف الفبركة في مقاطع الفيديو أو الصور بشكل فعال؟ ومتى أقوم بهذا الدور؟ كيف يمكن قياس "النقطة الحرجة"؟ كل هذه الأسئلة هي تحديات يواجهها من يعمل في بيئة مليئة بالمعلومات. إنه أمر معقّد.

دورة حياة التلاعب في الإعلام

جوان دونوفان

الدكتورة جوان دونوفان: هي مديرة قسم الأبحاث في مركز شورنستين للإعلام والسياسة والسياسات العامة التابع لكلية كينيدي في جامعة هارفارد.

في عصر تحظى فيه منصات تقنية عالمية معدودة وذات تأثير هائل بالقدرة على زعزعة الوسائل التقليدية التي كانت تعتمد عليها المجتمعات في الحصول على المعلومات، فإن عمليات التلاعب بالإعلام وحملات المعلومات المضللة تمثّل تحديًا صارخًا لكافة المؤسسات السياسية والاجتماعية.

فالمحتوى المضلل والفبركات التي تنتشر عبر أطراف متعددة تتبع جهات سياسية، أو علامات تجارية، أو حركات اجتماعية، أو حتى أطراف مجهولة الانتماءات، طوّرت تقنيات جديدة؛ بغية التأثير على الحوارات العامة وإثارة القلاقل على نطاق محلي أو وطني أو حتى عالمي.

وثمة اتفاق عريض بأن التلاعب والتضليل في الإعلام من المعضلات الحقيقية التي تواجه المجتمعات اليوم. لكن تعريف المعلومات المضللة والتلاعب الإعلامي وكشف ذلك وتوثيقه ودحضه ما يزال صعبًا، ولاسيما أن الهجمات باتت تستهدف قطاعات مهنية مختلفة مثل الصحافة والقانون والتكنولوجيا.

لذا فإن فهم التلاعب الإعلامي باعتباره نشاطًا ذا نمط ما سيكون خطوة أولى لا غنى عنها في العمل على التحقيق بشأن الظاهرة وفضحها والحد من ضررها.

تعريف التلاعب الإعلامي والمعلومات المضللة

لتعريف التلاعب الإعلامي يلزمنا أولًا أن نشرّح المصطلح بجزأيه:
فالإعلام في مفهومه الأكثر عمومًا هو وسيلة للتواصل. والأمثلة عليه هي النصوص والصور والمحتوى الصوتي والمرئي عبر الأوساط المادية أو الرقمية. وعند دراسة الإعلام، فإن أي أثر يصلح استخدامه دليلًا مسجلًا على حادثة ما. ومن الأهمية بمكان أن نشير إلى أن ثمة أطرافًا تنشئ المحتوى الإعلامي بهدف نقله إلى الآخرين. وبناء على ذلك، فإن الإعلام ينقل جزءًا من المعنى إلى الجمهور المستهدف، لكن تفسير هذا المعنى دائمًا ما يكون علائقيًا ومعتمدًا على سياق انتشاره وتلقّيه.

ادّعاء أن محتوًى إعلاميًا ما خاضع للتلاعب يعني تجاوز الفكرة البسيطة القائلة بأن المحتوى الإعلامي صادر عن طرف يرغب في نقل بعض المعاني المقصودة.

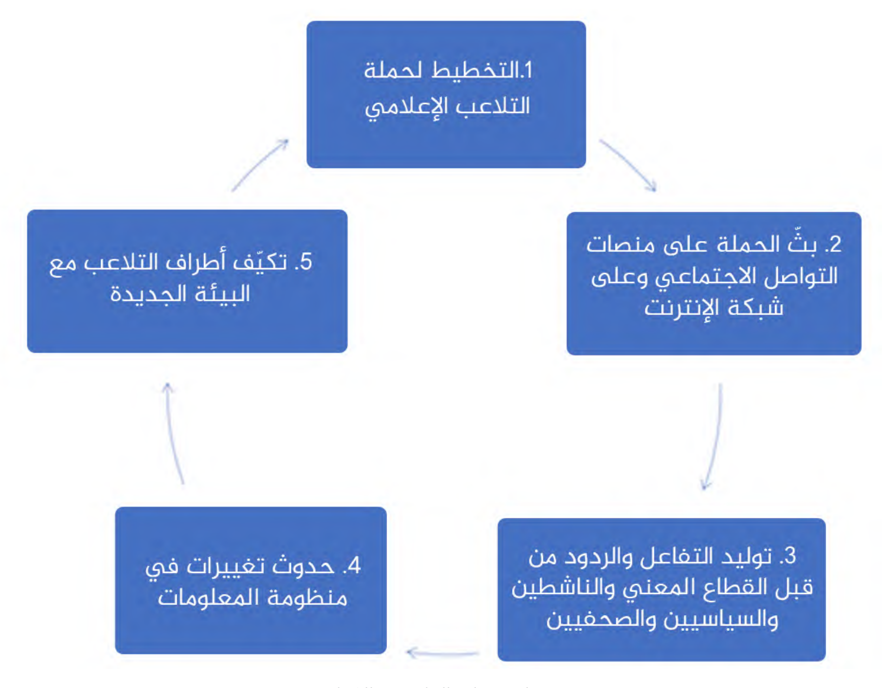
والتعريف المعجمي للتلاعب يشير إلى العبث بوسيلة فنيّة أو غير نزيهة بغية خدمة هدف ما. ومع أنه قد يصعب أحيانًا معرفة الهدف الدقيق وراء مادة إعلامية معينة، إلا أنه يسع المحققين تعقب التفاصيل المرتبطة بنشرها عبر طرح الأسئلة الأساسية عمّن أنشأها؟ ومتى؟ وأين؟ وكيف؟ بغية تحديد ما إذا كانت أساليب التلاعب قد وُظّفت بالفعل وكانت جزءًا من عملية نشر المحتوى.

وقد تشمل أساليب التلاعب التعتيم على هويّة طرف ما أو مصدر المحتوى، أو العبث بالمحتوى بغية إخفاء أو تغيير المعنى أو السياق، أو التأثير في الخوارزميات عبر اللجوء إلى عمليات تنسيق اصطناعية، مثل أدوات توليد البريد المزعج (السبام Spam) أو الحسابات الإلكترونية.

في هذا السياق تكون المعلومات المضللة شكلًا من أشكال التلاعب الإعلامي، وتعني الإنشاء والنشر المقصود لمعلومات مغلوطة لغايات

سياسية. ومن الضروري أن يتفق التقنيون والخبراء والأكاديميون والصحفيون وصناع السياسات على هذا التصنيف الموسوم بالمعلومات المضللة، وذلك لأن نجاح الجهود الرامية لمواجهة المعلومات المضللة يتطلب التنسيق فيما بين هذه المجموعات.

من ناحيتنا، فإن فريق البحث المعني بالتقنية والتغير الاجتماعي (Tech-nology and Social Change Research Team) في مركز شورنستين في كلية كينيدي بجامعة هارفرد، يعتمد على منهجية دراسة الحالة من أجل تحديد دورة حياة حملات التلاعب الإعلامي، وذلك من أجل تحليل النسق والحجم والنطاق لحملات التلاعب الإعلامي عبر تتبع المحتوى مكانيا وزمانيا، واستنتاج علاقات متعددة من خلال التنقيب في هذه الكتلة المتشابكة من المحتوى. وقد توصلنا عبر هذا العمل إلى وضع تصور عام عن دورة حياة حملات التلاعب الإعلامي، وهو تصور قد يكون في خدمة الصحفيين الذين يسعون إلى تحليل وتعقب وكشف عمليات التلاعب الإعلامي والمعلومات المضللة.



دورة حياة حملة التلاعب الإعلامي

دورة حياة حملة التلاعب الإعلامي تتألف من خمس مراحل يمكن في كل منها تحديد وتوثيق الأساليب التي يوظفها أطراف التلاعب الإعلامي باستخدام منهجيات نوعية وكمية. وتلزم الإشارة هنا إلى أن معظم حملات التلاعب الإعلامي لا يتم "اكتشافها" عبر هذا الترتيب بالضرورة، لذا فإنه من الممكن أثناء عملية البحث والتحقيق البحثُ عن أي من هذه المراحل ثم تعقب حركة هذه الحملة بالرجوع إلى مرحلة سابقة أو الانتقال إلى مرحلة تالية حسب النقطة التي انطلقت منها في دورة حياة الحملة.

دراسة حالة: "بلّغ عن الفساد"

فلندرس معًا التفاعل الذي حصل على وسائل التواصل الاجتماعي فيما يتعلق بالشكوى التي أثارها الشخص الذي سرّب معلومات بخصوص نشاط الرئيس الأمريكي دونالد ترمب المتعلق بأوكرانيا، من أجل تحديد كيفية تطوير حملة تلاعب إعلامي، وكيف أن السلوك الأخلاقي من قبل الصحفيين والمنصات في وقت مبكرة من دورة حياة حملات التضليل والتلاعب الإعلامي قد تساعد في فضحها وإبطال أثرها.



التخطيط والنشر (المرحلة 1 و2) - في المنظومة الإعلامية التي تؤمن بنظريات المؤامرة، تكون هويّة "مسرّب المعلومات" معلومة، ويكون اسمه متداولًا في المدونات وعلى تويتر وفيسبوك ويوتيوب ومنتديات الحوار. عندها، يبدأ استخدام الأسماء مكان الكلمات الرئيسية والوسوم (الهاشتاغ)، والتي تصبح نقاط بيانات تظهر في نتائج البحث. في هذه الحالة ظهرت جهود منسقة لنشر الاسم المزعوم وصورة الشخص، وبدا أن تداول الاسم محصور في "غرفة صدى" رقمية (Echo Cham-ber) لحسابات وكيانات ذات توجهات يمينية أو مؤمنة بنظريات المؤامرة. لكن وعلى الرغم من هذه الجهود من قبل مؤثرين ذوي توجهات "مؤامراتية" للتجييش نحو نشر اسم "مسرّب المعلومات" وتداوله في فضاءات النقاش العامة، فإنهم أخفقوا في ذلك وبقي الأمر محصورًا ضمن دوائرهم. فكيف حدث ذلك؟

تفاعل الصحفيين والناشطين وغيرهم (المرحلة 3) - في المقابل، أحجمت وسائل الإعلام المحسوبة على اليسار والوسط عن نشر الاسم وتداوله أو تداول الشائعات حول تحديد هويته. وكذلك فعلت وسائل الإعلام السائدة (Mainstream) عبر تجنب الخوض في اسم ذلك الشخص الذي سرّب المعلومات على وسائل التواصل الاجتماعي، بالرغم مما يشكّله الاسم من مادّة صحفية مغرية للصحفيين. وحتى في الحالات التي جرى فيها الإشارة إلى انتشار اسم مسرِّب المعلومات كان الحديث لا يخرج عن بيان أنّ تداول اسمه ليس إلا محاولة للتلاعب بطبيعة النقاش الدائر حول الشكاوى التي أثارها هذا الشخص، مع الاستمرار أيضًا في تفادي نشر اسمه. الأمر هنا يعود في جزء كبير منه إلى أخلاقيات المهنة، حيث يكون من واجب الصحفي حماية هوية المصادر، وهذا ينطبق على مسرّبي المعلومات (Whistleblowers).

التغيير في منظومة المعلومات (المرحلة 4) - في الوقت الذي أحجم فيه الصحفيون في وسائل الإعلام السائدة عن ذكر اسم مسرّب المعلومات، إلا أن الاسم المزعوم للمسرِّب قد بات كلمة بحث فريدة على محرك البحث، ما يعني أن من يبحث عن هذا الاسم (Eric Ciaramella)، سيجد قدرًا

غير قليل من المحتوى والمرتكز في معظمه على آراء مغرقة في نظرية المؤامرة. وبالإضافة إلى الموقف الأخلاقي الفعّال من قبل الصحفيين لوضع حدّ لقصة صحفية كان يمكن أن تشعل الكثير من التفاعل والزخم والزيارات، فإن منصات التواصل الاجتماعي بدأت بالفعل بضبط المحتوى الذي استخدم اسم مسرّب المعلومات، وعمدت يوتيوب وفيسبوك إلى حذف المحتوى الذي استخدم الاسم، ومنعت تويتر المحتوى المتعلق باسمه من التصدّر. أما جوجل فاستمر في إظهار اسمه في نتائج البحث التي تحيل إلى آلاف المواقع والمدونات التي تروج لنظريات المؤامرة.



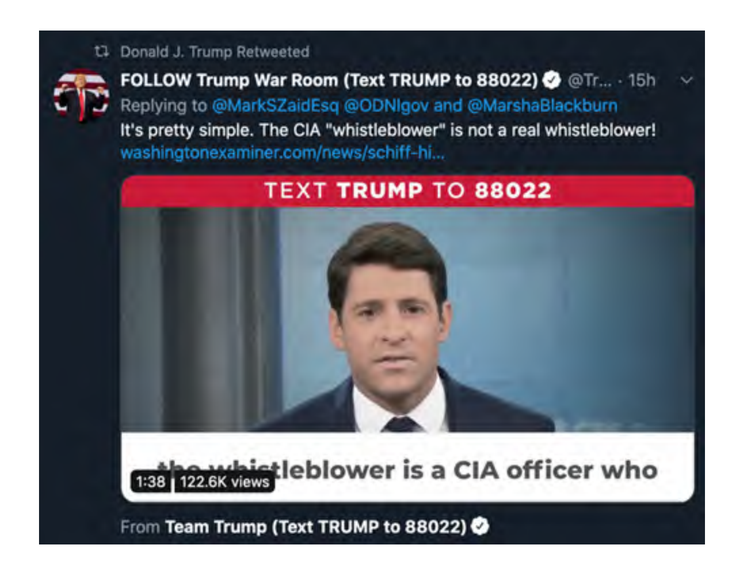
التكيف مع التعديلات في المنظومة (المرحلة 5) - انزعج الأطراف الذين وقفوا وراء هذه الحملة من المساعي التي حاولت منع انتشار المعلومات المضللة، ودفعهم ذلك إلى تغيير أساليبهم. فبدلًا من ترويج المحتوى الذي يشتمل على اسم مسرّب المعلومات، بدأوا بنشر صورة لرجل أبيض آخر (بلحية ونظارات) شبيهة بالصورة التي نشرت مسبقة مع الاسم. وانتشرت هذه الصور الجديدة مع سردية مؤامراتية حول

"الدولة العميقة" تذكر أن مسرّب المعلومات كان صديقًا لأحد أبرز أعضاء الحزب الديمقراطي، ولديه دوافع حزبية. لكن الصورة التي انتشرت لم تكن إلا صورة لألكساندر سوروس، ابن رجل الأعمال الملياردير والمهتم بالعمل الخيري جورج سوروس، والذي يعدّ هدفًا شهيرًا لنظريات المؤامرة.

وحين أخفق هذا الأسلوب أيضًا في جذب الانتباه الإعلامي، قام حساب الرئيس الأمريكي دونالد ترمب على تويتر والذي يتابعه 68 مليون متابع، بإعادة تغريد مقال يتناول اسم مسرب المعلومات المزعوم، ويتضمن تأكيدًا مزعومًا بأن "مسرب المعلومات في وكالة الاستخبارات الأمريكية ليس مسرب معلومات حقيقيًا!". التغريدة الأصلية ظهرت في حساب (@TrumpWarRoom)، وهو الحساب الرسمي والموثق لحملته الانتخابية. كان ذلك فقط كفيلًا بإثارة تغطية إعلامية مكثفة، شاركت بها أيضًا وسائل الإعلام السائدة، وحاولت جميعها إزالة أو تغطية الاسم المزعوم لمسرب المعلومات. وبدأ الناس على وسائل التواصل الاجتماعي بدعوة هذا الشخص إلى الحديث أمام مجلس الشيوخ الأمريكي ضمن الشهادات الخاصة بمحاكمة الرئيس الأمريكي، حيث ذُكر اسمه إلى جانب عدد من أهم الشهود المحتملين، ما وسّع من فرصة العثور على الاسم وتداوله حتى عند البحث عن أسماء الشهود الآخرين، وبهذا تبدأ حياة دورة أخرى من التلاعب الإعلامي.

تزايدت عمليات البحث عن اسم مسرب المعلومات وانتشرت الكثير من الأقاويل في مدونات خاصة بنظريات المؤامرة حول الدوافع الشخصية والمهنية لهذا الشخص في الإبلاغ عن أنشطة ترمب. وعادة ما يتراوح موقف الصحفيين الذين يغطون مثل هذه التغريدات بين مناقشة عمليات الترهيب التي يتعرض لها الشاهد، والإشارة إلى أن مثل هذه العمليات قد تثير الخوف لدى آخرين من القيام بأفعال مشابهة، أو اللعب على وتر الفضول وتناول الجدل حول دوافع الرئيس الأمريكي نفسه لفضح الهوية المزعومة لمسرب المعلومات. وهنا تلزم الإشارة إلى أنه ورغم أن موقف المؤسسات الإعلامية الساعي إلى مساءلة النخب هو موقف جدير

بالثناء، إلا أن المهمة تغدو مستحيلة ما لم تتخذ منصات التواصل الاجتماعي خطوات تمنع استغلالها كأدوات في حملات التلاعب الإعلامي والتضليل من قبل السياسيين.



توثيق دورة حياة حملات التلاعب الإعلامي

حاولت الأطراف التي تقف وراء حملات التلاعب الإعلامي تغيير قواعد اللعبة، وسعت إلى بث الاسم والصور على وسائل التواصل الاجتماعي كخطوة أولى لجذب اهتمام وسائل الإعلام الكبرى والسائدة إلى الطعم، الذي يساعد في انتشاره طريقة عمل منصات التواصل. لكن القرارات والإجراءات التي اتخذتها المنصات والصحفيون بينت أن محاولة فضح الهوية المزعومة لمسرب المعلومات والتسبب برواجها في وسائل الإعلام السائدة قد أخفقت، ولم تنجح إلا حين قامت شخصيّة مؤثرة لا يمكن للإعلام تجاهلها بتغيير مسار القضيّة. ورغم أن العديد من وسائل الإعلام تسعى إلى الالتزام بالقواعد الأخلاقية الناظمة لعملها، إلا أن وسائل التواصل الاجتماعي قد باتت سلاحًا لمن يملكون السلطة أصلًا، وتمكينهم من فرض الأجندات الإعلامية أو إتاحة حيّز أوسع لانتشار نظريات مؤامرة قد تشكل خطرًا على المجتمع.

لكن هذا لا يمنع من التأكيد عمومًا على أن دراسة الحالة هذه تعد خطوة كبيرة إلى الأمام ضمن الجهود الرامية إلى محاربة المعلومات المضللة، إذ التزم الصحفيون في تجنب أن يكونوا أداة للترويج للمعلومات المضللة حتى لو كان ذلك من باب محاولة دحضها، إضافة إلى دور شركات منصات التواصل الاجتماعي في استشعار الواجب بالتدخل لمنع انتشار المعلومات المغلوطة. هذا التحوّل العام في هذه الحالة يمثل فرصة واعدة، بالرغم من استمرار غياب القدرة على مساءلة النخب بالشكل الكافي. ويبقى على عاتق الصحفيين والباحثين مهمة بالغة الخطورة في الاستمرار بتعقب حملات التلاعب الإعلامي وتوثيقها ودحضها، خاصة في بيئة مشحونة سياسيًا، حيث تعترض محاولات الكشف عن أي حملة مضللة احتمال التعرض لهجمات واسعة من التصيّد والتنمّر. إن التعاطي مع محتوى حملات التضليل وسياقها يتطلب منا جميعًا الحرص على التوثيق التفصيلي الدقيق لكيفية انطلاق هذه الحملات وتطورها وانتهائها، والتنبه إلى أن أي نهاية لحملة ما قد يكون في حالات كثيرة إشارة إلى بداية جديدة لها.

الفصل الأول: التحقق من الحسابات على وسائل التواصل الاجتماعي

براندي زادروزني

براندي زادروزني هي صحفية استقصائية مع شبكة NBC News، مختصة بمواضيع المعلومات المضللة والتلاعب الإعلامي والتطرف على شبكة الإنترنت.

لا يخلو أي تقرير أعمل عليه من البحث المعمق في وسائل التواصل الاجتماعي، سواء كنت أستقصي عن المزيد من المعلومات عن شخصية ما، أم أتتبع خبرًا عاجلًا، أم أقوم بعمليات استقصائية أكثر عمقًا. فوسائل التواصل الاجتماعي تعدّ إحدى أفضل السبل لمعرفة الكثير عن حياة الشخص، وعائلته، وأصدقائه، وعمله، وتوجهاته السياسية، وعلاقاته، إضافة إلى كون هذه المنصات نافذة على أفكار ذات طبيعة سرية أو هويات خفية في العالم الرقمي.

نحن في عصرٍ مثير جدًا من وجهة نظرٍ صحفية، فالناس يعيشون حياتهم بشكل متزايد على الإنترنت، وتتوفر الكثير من الأدوات التي تساعد في البحث في وسائل التواصل الاجتماعي. وفي الوقت ذاته، يتزايد الحرص بين المستخدمين العاديين والأطراف ذوي الدوافع الخبيثة على محو آثارهم الرقمية. كما أننا في المقابل نشهد بعض التغيرات على وسائل التواصل الاجتماعي، إذ استجابت فيسبوك مؤخرًا على سبيل المثال إلى الانتقادات السلبية في الإعلام حول خروقات الخصوصية والسماح لانتشار الأيديولوجيات المتطرفة، وعمدت إلى حجب الأدوات التي كان يعتمد عليها الصحفيون والباحثون من أجل تفحص المحتوى وتحديد هويات الأشخاص.

في هذا الفصل سأستعرض عددًا من أهم المنهجيات في التحقق من الحسابات على وسائل التواصل الاجتماعي. الأدوات التي سأتحدث عنها هنا هي تلك المتوفرة للاستخدام حتى الآن، لكن قد تُقْدم فيسبوك على تعطيلها كما قد تَظهر أدوات أخرى أفضل منها.

ويفترض أن أي صحفي مهني لديه عملياته وأدواته الخاصة التي يفضل استخدامها للوصول إلى النتائج المرجوّة، لكن لا شكّ في أن الإصرار واستخدام الأساليب التقليدية (الافتراضية) كفيلة بتقديم أفضل النتائج. فلا بدّ أن يكون لدينا الاستعداد، والرغبة، لقراءة آلاف التغريدات، والنقر على آخر النتائج في محرك البحث، والغوص عميقًا في منصات التواصل الاجتماعي إن كنا جادين حقًا في السعي للوصول إلى أدلة مفتاحية أولية تساعدنا في الإجابة على سؤال: "لمن ينتمي هذا الحساب؟".

اسم المستخدم

قد لا يتوفر لدينا أحيانًا سوى اسم المستخدم (Username)، ولا بأس في ذلك، لأن هذه غالبًا ما تكون هي نقطة البداية. كانت هذه هي الحالة التي تعاملنا معها لمن كان حينها نائبًا عن الحزب الجمهوري في ولاية نيوهامبشير، والذي أنشأ واحدة من أكثر الجماعات الذكورية الرقمية شهرة وسوء سمعة على منصة "ريديت" (Reddit). وقد بدأ التحقيق الذي كشف عن الشخص وراء هذه الجماعة التي أطلقت على نفسها اسم "The Red Pill" من اسم المستخدم (pk_atheist).

Welcome to the Red Pill (self.TheRedPill)
12 submitted 2 years ago * by pk_atheist

I'm going to discuss briefly what my intention is for this subreddit.

I'm Desmond, and I've been active in both the Men's Rights and the Seduction subreddits. They're both wildly popular subs, but both have major failings that I've slowly identified. They both operate subtly under the feminist imperative. Group-think at both tend to fail to grok the importance of coming to terms with objective reality - something the manosphere has termed "taking the red pill."

يلتـزم البعـض باسـم مسـتخدم واحـد أو اثنيـن علـى عـدة منصـات وخدمـات للبريـد الإلكترونـي، بتغييـرات طفيفـة أحيانًـا. أمـا الشـخص المهتـم بالحفـاظ علـى سـريّته وأمنـه الرقمـي، مثـل النائـب عـن ولايـة نيوهامبشـر، فسـيعتمد على أسماء مستخدم مختلفة في كل مرّة.

[-] pk_atheist [S] 2 points 3 years ago
I don't think we can grow if we ever go private. It goes without saying, you should invest in a decent throwaway that cannot be traced back to you.
permalink embed parent

وأيًّـا كانـت الحالـة، فلدينـا بعـض المواقـع الإلكترونيـة التـي يلزمـك اسـتخدامها للبحث فيها عن اسم المستخدم موضوع التحقيق.

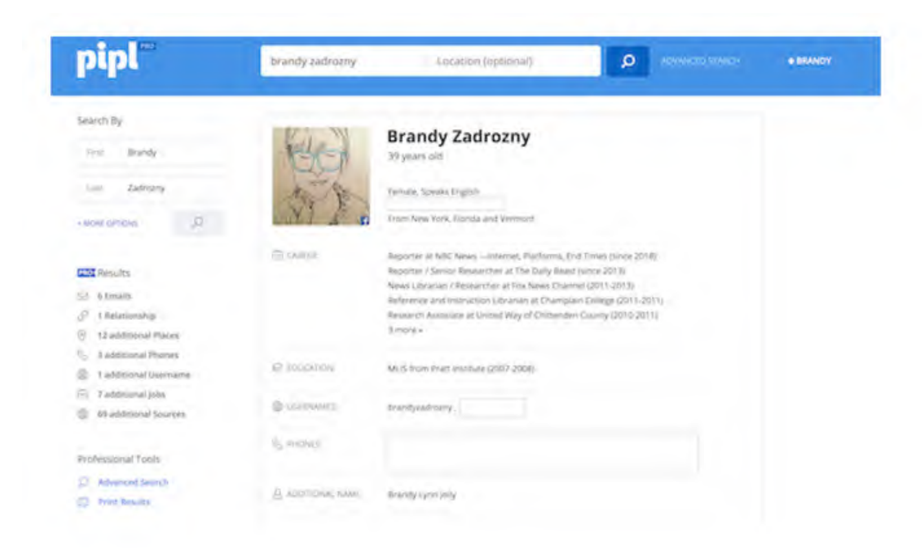
فـي البدايـة أقـوم بالبحـث عـن اسـم المسـتخدم فـي جوجـل. ولا بـد أن العديـد مـن الأشـخاص، خاصـة مـن الشـباب الذيـن لا يفضلـون الظهـور علـى منصـات التواصـل الاجتماعـي الكبيـرة، سـيتركون عـادة أثـرًا يـدل عليهـم، حتـى فـي أكثـر الأماكـن غيـر المتوقعـة، مثـل التعليقـات فـي موقـع أو منتـدى مـا، أو المراجعـات لمنتـج أو كتـاب، وغيـر ذلـك ممـا يسـاعد فـي التوصـل إلى معلومات إضافية وحسابات أخرى.

ويمكـن بالإضافـة إلـى البحـث فـي جوجـل الاعتمـاد علـى بعـض الخدمـات المدفوعـة، وتوفرهـا بعـض غـرف الأخبـار للعامليـن لديهـا. هنالـك مثـلًا أداة "نيكسـيس" (Nexis)، وهـي أداة ممتـازة للبحـث فـي السـجلات العامـة ووثـائق المحاكـم، ولكنهـا مـع الأسـف ليسـت مناسـبة للبحـث عـن عناويـن البريـد الإلكترونـي أو أسـماء المسـتخدمين، كمـا أنهـا لا تفيـد سـوى فـي البحث عن الأشخاص في الولايات المتحدة الأمريكية.

وثمـة منصتـان أخريـان همـا "بيبـل" (Pipl)، وسـكوبناو (Skopenow)، وهمـا مـن أفضـل الأدوات التـي تعاملـتُ معهـا فـي الربـط بيـن معلومـات مـن المصـادر التقليديـة، مثـل أرقـام الهواتـف وسـجلات الملكيـة، مـع المعلومـات الرقميـة مثـل عناويـن البريـد الإلكترونـي وأسـماء المسـتخدم، وكلا التطبيقيـن

مفيدٌ للبحث في كافة الدول.

كما توفر محركات البحث المدفوعة هذه عادة إمكانية البحث في سجلات الهاتف والملكية، كما يمكن أن تقدم معلومات عن حسابات على فيسبوك ولينكد إن حتى بعد قيام أصحابها بإغلاقها. كما أنها تساعد في الربط بين حسابات في أماكن منسيّة غالبًا، كالمدونات والمنتديات القديمة أو حتى قائمة طلبات من أمازون (Wishlist)، وهذا يساعد في اكتشاف المزيد عن قراءات الشخص واهتماماته وقراءاته وحتى مشترياته. كما ستكتشف في مثل هذه الخدمات بعض الروابط غير المفيدة، وهذا ما يجعلها نقطة بداية جيدة في عملية التحقق قبل الانتقال إلى وسائل أخرى.



بعد العثور على اسم مستخدم أو عنوان بريد إلكتروني أشك بارتباطه بالموضوع الذي أبحث عنه، أستخدم أداة متوفرة على الإنترنت مثل "Namechk" أو "Namecheckr"، لأفحص توفر اسم المستخدم عبر المنصات المختلفة.

هذه الأدوات مصممة لتكون وسيلة سهلة للعاملين في مجال التسويق لفحص ما إذا كان الاسم الذي يرغبون في استخدامه وتسجيله مستخدم من قبل على

المنصـات المختلفـة. لكنهـا أيضًـا مفيـدة فـي فحـص تواجـد اسـم المسـتخدم الـذي تبحـث عنـه علـى منصـات أخـرى. مـن الضـروري أن نتذكـر أن وجـود اسـم المسـتخدم علـى منصـة أخـرى لا يعنـي أنهـا جميعها بالضـرورة تعود للمسـتخدم ذاته، لكنها مع ذلك نقطة بداية مهمّة للبحث عبر المنصّات المختلفة.



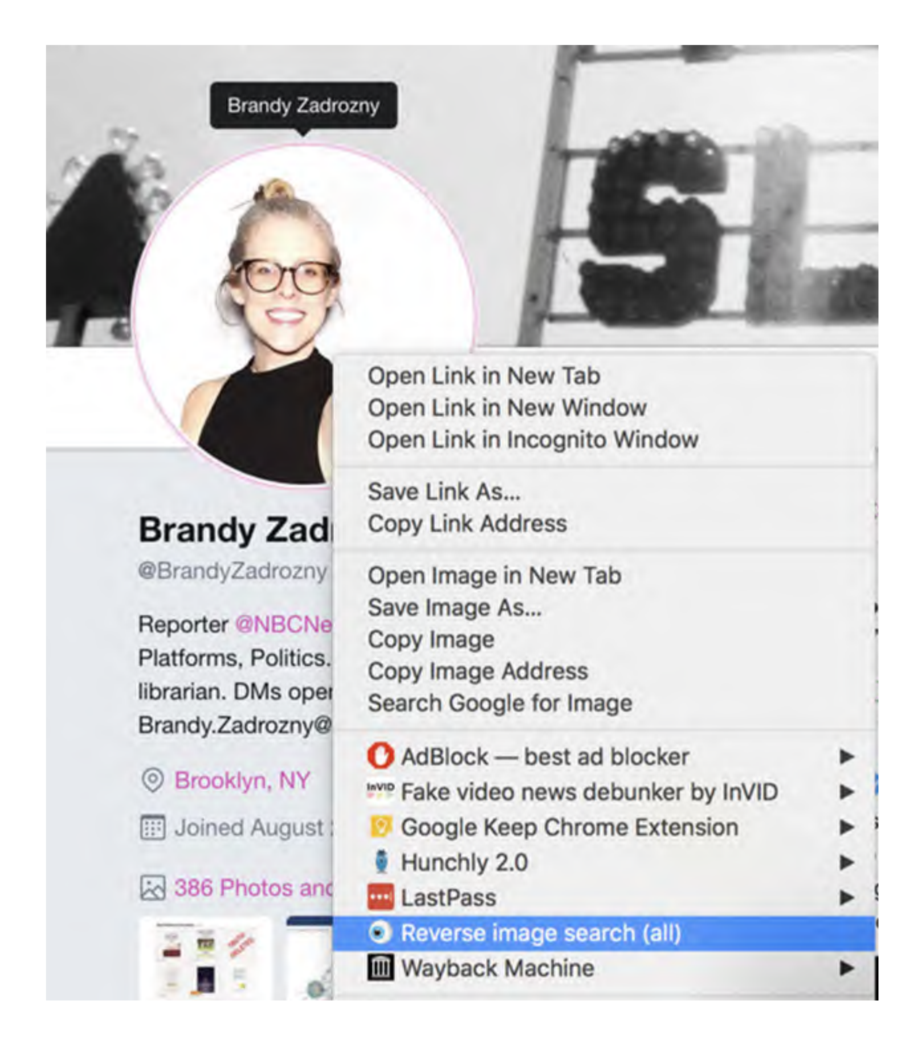
أما للبحـث بشـكل أعمـق عبـر اسـم المسـتخدم، فيكمـن الاعتمـاد علـى موقـع (haveibeenpwned.com)، وموقـع (Dehashed.com)، وهمـا موقعـان يسـاعدان فـي البحـث عـن أي عمليـة خـرق للبيانـات الخاصـة بالمسـتخدم ومعلوماتـه، ويوفـران طريقـة سـريعة للتأكـد مـن صحـة عنـوان بريد إلكتروني والحصول على خيوط أدلة جديدة.

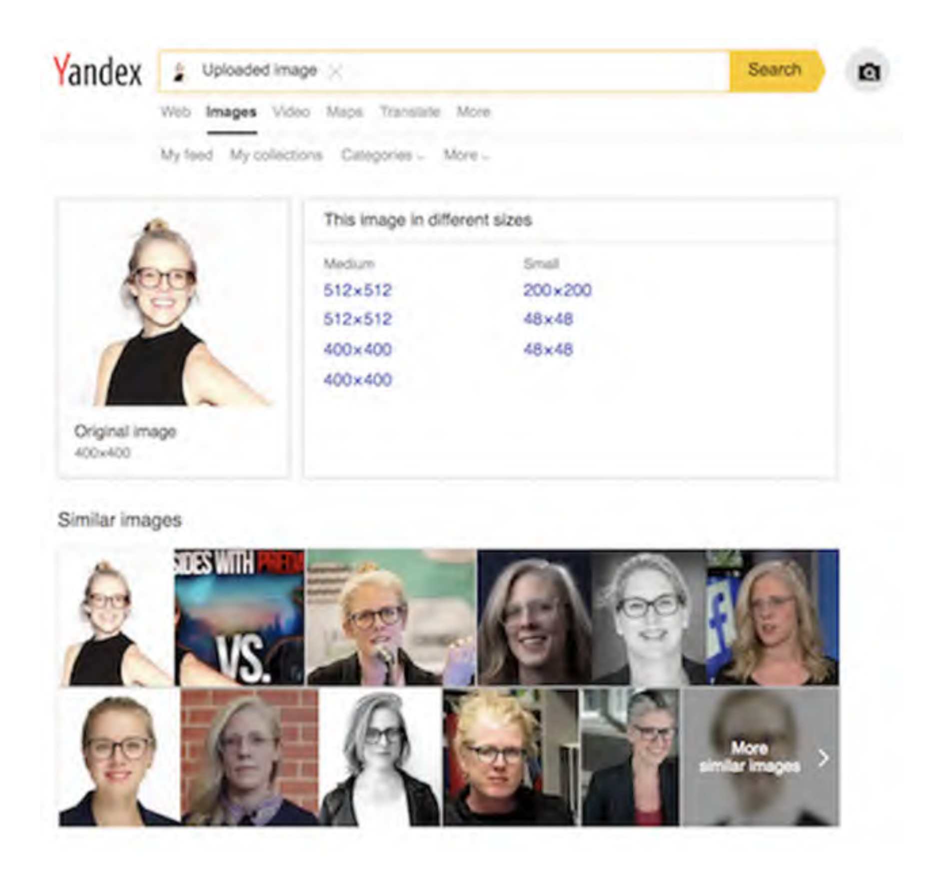
الصور

قـد لا يكفـي اسـم المسـتخدم دائمًـا لتقديـم معلومـات أوليـة وافيـة ينطلـق منهـا الصحفـي، وعندهـا يمكـن الانتقـال إلـى الصـورة، وهـي العنصـر الأكثـر إقناعًـا دومًـا وتغنـي عـن الكثيـر مـن الـكلام. صـورُ الحسـابِ الشـخصيةُ هـي

طريقة ثانية من أجل التحقق من هوية الشخص عبر الحسابات المختلفة.

يمكن بالتأكيد الاستفادة من محرك البحث بالصور لدى جوجل، لكن ثمة محركات أخرى تقدم نتائج أفضل، مثل موقع Yandex الروسي. كما أستخدم شخصيًا إضافة (Extension) متوفرة على جوجل كروم، وهي (Reveye)، والتي يمكن عبرها وخلال نقرة واحدة على الصورة البحث عن مثيلاتها عبر المنصات المختلفة، مثل جوجل وبينغ (Bing)، وياندكس (Yandex)، وتينآي (Tineye). هنالك إضافة أخرى أيضًا للبحث عبر الصور فيها خاصية التقاط جيدة (Capture) والتي تتيح كذلك إمكانية البحث عن صورة داخل صورة.



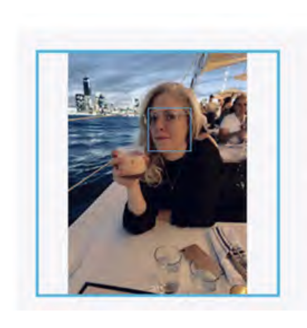


هنالك بالتأكيد بعض المشكلات المتعلقة بالبحث العكسي عن الصور؛ فالخدمات التي أشرنا إليها أعلاه لا تعطي نتائج جيدة في البحث عن الصور على تويتر، وجميعها غير مجدية في البحث عن صور من إنستغرام أو فيسبوك.

وفي كثير من الأحيان أكون مهتمة بالبحث عن صور مختلفة للأشخاص، وكثيرًا ما حدّقتُ في الشاشة طويلًا لأقارن بين صورتين لأتأكد إن كانتا للشخص ذاته أو لا، وأستعين بزملائي للوصول إلى إجابة ما.

لا أستطيع بالتأكيد أن أثق بعيني، لكني مهتمة باكتشاف بعض السمات المحددة عبر صور مختلفة، مثل البثور أو الشعر على الوجه أو أي سمة مميزة أخرى. بدأت مؤخرًا بالاستفادة من أدوات التعرف على الوجوه،

مثل Face++ والتي تتيح تحميل صورتين للمقارنة بينهما وتساعد في تحديد ما إذا كانت الصورتان عائدتين للشخص ذاته. في الأمثلة التالية ستجد أن هذه الأداة قد نجحت في تحديد أني صاحبة الصورتين، رغم أن بينهما فرقًا يبلغ 10 سنوات. كما ربط بين صور زميلي على حساباته على فيسبوك وتويتر، ونوّهت كذلك إلى أنّه شخص مختلف عن الممثل بين ستيلر (Ben Stiller).











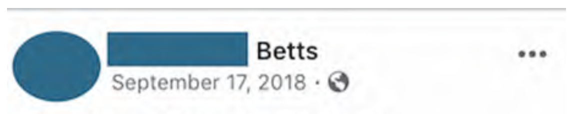

في حال كنت تسعى وراء حسابات لبعض المتصيدين أو الذباب الإلكتروني، فستجد أنهم يبذلون جهودًا أكبر في إخفاء صورهم، هذا

إن لـم يكونـوا يسـتخدمون صـورًا مزيَّفـة. هنـا قـد يلـزم تحريـر الصـورة وقلبُهـا لمحاولـة التوصـل إلـى شـكلها الأصلـي قبـل عمليـة التحويـر التـي خضعت لها.

مـن المعـروف كذلـك أن صـور الحسـابات ليسـت دومًـا صـورًا شـخصية، فالبعـض يتعامـل بحـرص أكبـر مـع مسـألة خصوصيتـه وخصوصيـة أسـرته، ويفضـل اسـتخدام صـور لأشـياء يحبهـا أو يفخـر بهـا. لقد تمكنـتُ فـي عمليات سـابقة مـن تحديـد بعـض الأشـخاص عبـر الربـط بيـن صـور مختلفـة، كالسـيارات أو البيـوت أو الحيوانـات الأليفـة. بهـذه الطريقـة؛ قـد تفيـد هـذه الصـور أيضًـا فـي الربـط بيـن حسـابات مختلفـة علـى منصـات التواصـل الاجتماعـي، وبنـاء الشـبكة المطلوبـة حـول الموضـوع المسـتهدف. ويعـد هـذا الإجراء أساسيًّا عند التحقق من حسابات وسائل التواصل الاجتماعي.

فعلـى سـبيل المثـال، فـي حـال كنـا نحـاول التأكـد مـن حسـابات وسـائل التواصـل الاجتماعـي لشـخص قـام بإطـلاق النـار علـى تسـعة أشـخاص علـى مدخـل بـار فـي مدينـة دايتـون فـي أوهايـو. لقـد كشـف حسـابه علـى تويتـر شـيئًا عـن الأيديولوجيـا السياسـية التـي يعتنقهـا، لكـن اسـم المسـتخدم الخـاص بـه (iamthespookster@) كان مميـزًا ولا يتقاطـع مـع الاسـم الحقيقـي الذي أفصحت عنه السلطات.

لقـد كان أحـد ضحايـا هـذه الحادثـة أخًـا للقاتـل، وهـو رجـل عابـر جنسـيًا، واسـمه لـم يـرد فـي السـجلات العامـة، ولـم يفصـح عـن هويتـه الجنسـية، وهـو مـا عقّـد عمليـة البحـث عـن أيـة خيـوط إضافيـة. لكـن مـا كان لافتًـا هـو وجـود صـور لكلـب علـى حسـابه الشـخصي وحسـابات عائلتـه، ويبـدو أن هـذا الكلـب هـو الصـورة التـي اسـتخدمت علـى حسـاب أخيـه العابـر جنسـيًا الـذي لـم يـرد في التقارير.

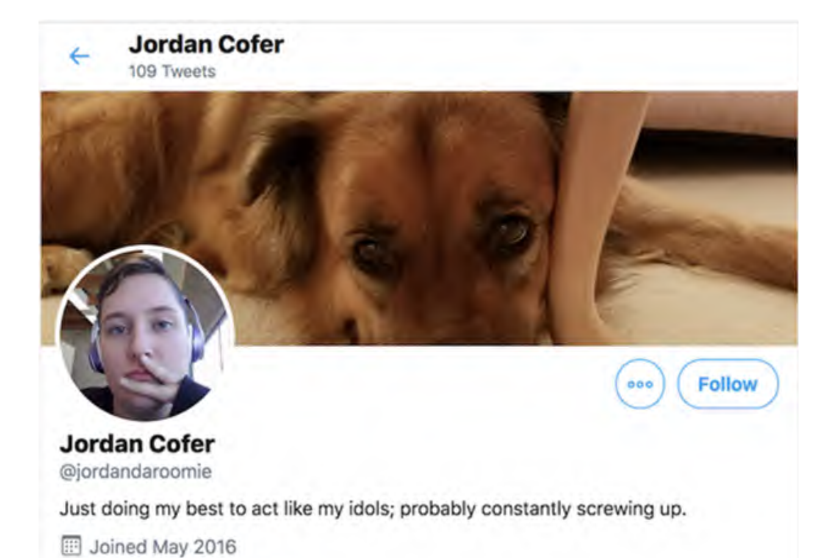

Betts
September 17, 2018 ·
Sometimes I forget how big he is.

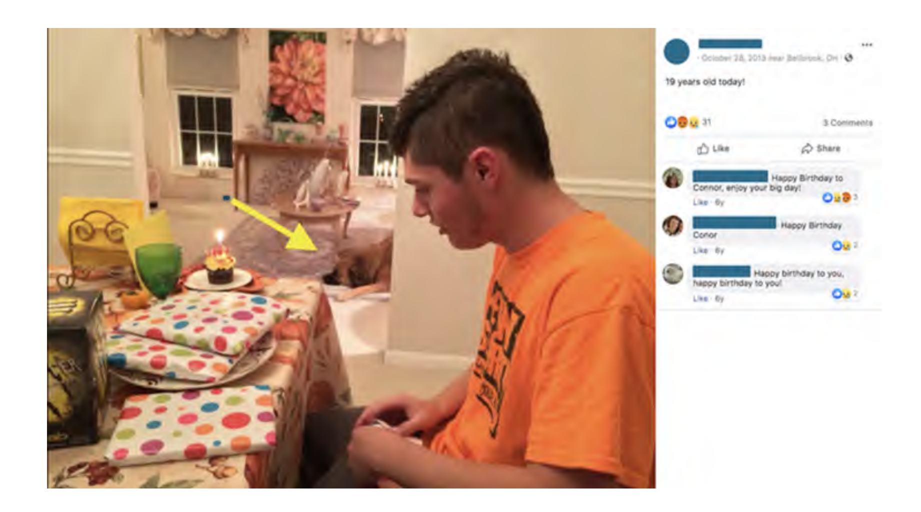





5




Jordan Cofer
109 Tweets
Follow
Jordan Cofer
@jordandaroomie
Just doing my best to act like my idols; probably constantly screwing up.
Joined May 2016
25 Following
101 Followers



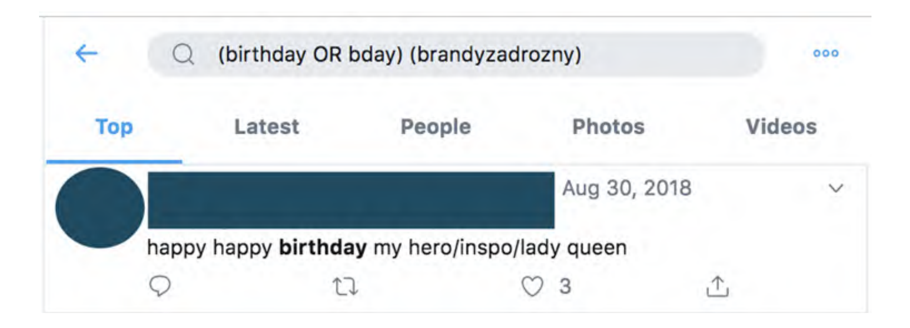
لم يكن الكلب هو التفصيل الوحيد المفيد في الصور السابقة. فالصورة وصلتنا عبر والد القاتل، وساعدتنا في التحقق من حساباته الشخصية وحسابات أفراد أسرته.

إن كنت تمتلك حسابًا على فيسبوك أو تويتر، فبوسعي على الأرجح أن أخبرك بتاريخ ميلادك، حتى لو كنت تحجب هذه المعلومة في ملفك الشخصي أو لم تذكر ذلك بنفسك. فتاريخ الولادة عادة ما يكون أول معطىً من المعلومات التي تقدمها الشرطة في مواقف الأخبار العاجلة. ومن الطرق التي يمكن الاعتماد عليها في التحقق من ربط الاسم بالحساب على وسائل التواصل الاجتماعي هو الذهاب إلى المنشورات في ذلك التاريخ الذي ذكرته الشرطة، فربما ستجد عبارات التهنئة والمباركة بذكرى ميلاده. وحتى لو لم تجد، فيمكن أن تجد ذلك على حسابات المقربين منه، مثل أمه أو أبيه، والذين يكتبون عادة عبارة تهنئة عن أبنائهم في ذكرى ميلادهم (مثلما نجد في صورة Connor Bett). وينطبق ذلك على تويتر أيضًا، لأن الجميع عادة يحبون التهنئة بذكرى ميلادهم.





لكـن الأسـهل هـو العثـور علـى منشـور كهـذا فـي تويتـر، وذلـك لأن تويتـر تتيـح خاصيـة البحـث المتقدم، وتتفـوق بذلـك علـى معظـم المنصـات الأخـرى. ورغـم أنـي شـخصيًا لا أفصـح عـن يـوم ميـلادي، ولـم أفعـل ذلـك يومًـا علـى مـا أذكـر، إلا أنـي وجـدت علـى حسـابي تغريـدة تهنئـة مـن زميـل عزيـز، وكشف عن ذلك.



يمكن أيضًا بالإضافة إلى مناسبة ذكرى الميلاد، البحث عبر الذكرى السنوية للزواج أو الوفاة، أو التخرج، أو أي حدث مهمّ آخر، باعتبار أن ذلك كلّه يكون موضوع احتفال وتفاعل على حساب الشخص على وسائل التواصل الاجتماعي.

يمكن بسهولة البحث عن الكلمات المفتاحية وغيرها من فلاتر البحث مع أدوات البحث على فيسبوك. قد لا تحصل على القدر المطلوب من النتائج باستخدام هذه الأدوات، وذلك بسبب سياسات الخصوصية، لكنها متوفرة، وأفضّل عادة استخدام (whopostedwhat.com).

العلاقات

يمكنك الحكم على الشخص عبر النظر في قائمة معارفه على وسائل التواصل الاجتماعي، كما يمكن معرفة الكثير عن حياته وتوجهاته عبر تحديد الأشخاص الذين يعرفهم ويتفاعل معهم على منصات التواصل الاجتماعي.

حين انضممت إلى تويتر، طلبت من زوجي وصديقي المفضل أن ينشئ كل منهما حسابًا على المنصة أيضًا، كي يتابعوني. أفكر بهذا وأنا أبحث في بعض الحسابات الخاصة بالعمل. المنصات التي ننضم إليها لا تريدنا أن نبقى هنالك معزولين وحدنا، لذلك حين تنشئ حسابًا، فإن الخوارزمية تعمل على الفور، بالاستفادة من قائمة الاتصال على هاتفك أو على

حسابات أخرى، وعبر تحديد موقعك، وغير ذلك من العوامل، ستبدأ المنصة باقتراح إضافة العديد من الحسابات ومتابعتها.

وانطلاقًا من هذه الملاحظة، يمكن استنتاج الكثير عن الشخص عبر النظر في قائمة أول المتابعين والأصدقاء. أداة TweetBeaver تساعد في التحقق من الروابط بين حسابات كبيرة وتنزيل بعض البيانات مثل الخط الزمني وقائمة المفضلات في حسابات أصغر. أما للحصول على بيانات أكبر، فسأكون مضطرة للاعتماد على مطوّر محترف مع إمكانية دخول إلى واجهة برمجة التطبيقات (API).

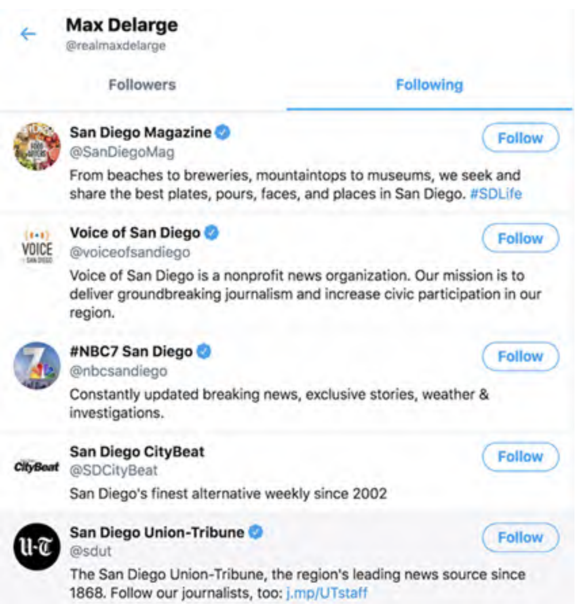
فلنأخذ مثلًا حساب (ذا كولومبيا بيوغل The Columbia Bugle)، وهو حساب على تويتر يديره شخص مجهول الهوية ويروج لأيديولوجيا اليمين المتطرف، يتبجّح كثيرًا بأن حساب الرئيس الأمريكي دونالد ترمب نفسه قد أعاد تغريد اثنين من منشوراته.



من خلال البحث في هذه الأداة سنجد أن من أول المتابعين لماكس ديلارج (Max Delarge) -وهو حساب يدعي أنه محرر في موقع "ذا كولومبيا بيوغل"- هم حسابات أخبار من سان دييغو وحسابات رياضية من سان دييغو أيضًا.

وبما أن العديد من تغريدات حساب "كولومبيا بيوغل" تشتمل على مقاطع فيديو من مهرجانات خطابية لترمب في سان دييغو وفعاليات من جامعة كاليفورنيا سان دييغو، فإنه يكون بوسعنا أن نفترض بثقة كبيرة أن الشخص الذي يدير الحساب يعيش قرب سان دييغو.


Follow
Max Delarge
@realMaxDelarge
Co-Editor of The Columbia Bugle. Still got the scars of #NeverTrump, but im on the #TrumpTrain for good, unless he lights the train on fire
United States
Joined July 2016
22 Following
0 Followers


Max Delarge
@realmaxdelarge
Followers
Following
San Diego Magazine
@SanDiegoMag
From beaches to breweries, mountaintops to museums, we seek and share the best plates, pours, faces, and places in San Diego. #SDLife
Follow
Voice of San Diego
@voiceofsandiego
Voice of San Diego is a nonprofit news organization. Our mission is to deliver groundbreaking journalism and increase civic participation in our region.
Follow
#NBC7 San Diego
@nbcsandiego
Constantly updated breaking news, exclusive stories, weather & investigations.
Follow
San Diego CityBeat
@SDCityBeat
San Diego's finest alternative weekly since 2002
Follow
San Diego Union-Tribune
@sdut
The San Diego Union-Tribune, the region's leading news source since 1868. Follow our journalists, too: j.mp/UTstaff
Follow



فـي عمليـات البحـث الجديـدة أفضّـل دومًـا أن أبـدأ مـن تاريـخ بـدء أي حسـاب أتقصّـى عنـه، والانطـلاقَ مـن تلـك النقطـة. يمكـن القيـام بهـذه العملية يدويًّـا، أو عبـر استخدام إضافـة علـى المتصفـح للمسـاعدة فـي تمريـر الصفحـة (Auto-scroll). كمـا يمكـن اسـتخدام آليـة البحـث المتقدمـة فـي تويتـر مـن أجـل اختصـار الفترة الزمنية وتحديدها بالأشهر القليلة الأولى لإنشاء الحساب.

Advanced search
Search

Accounts

From these accounts
@ColumbiaBugle
Example: @Twitter · sent from @Twitter

To these accounts
Example: @Twitter · sent in reply to @Twitter

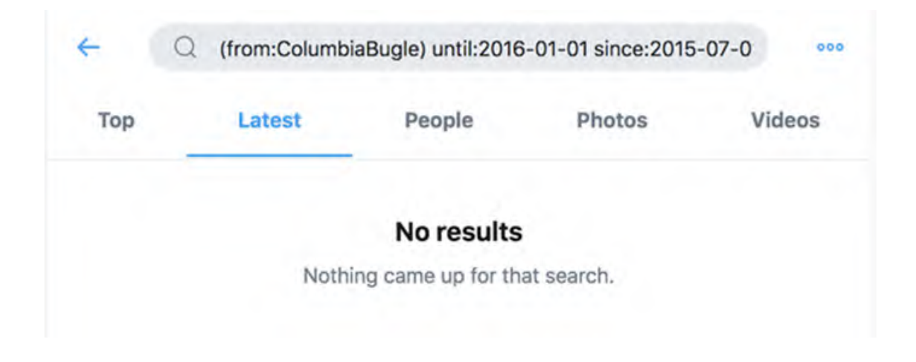
Mentioning these accounts
Example: @SFBART @Caltrain · mentions @SFBART or mentions @Caltrain

Dates

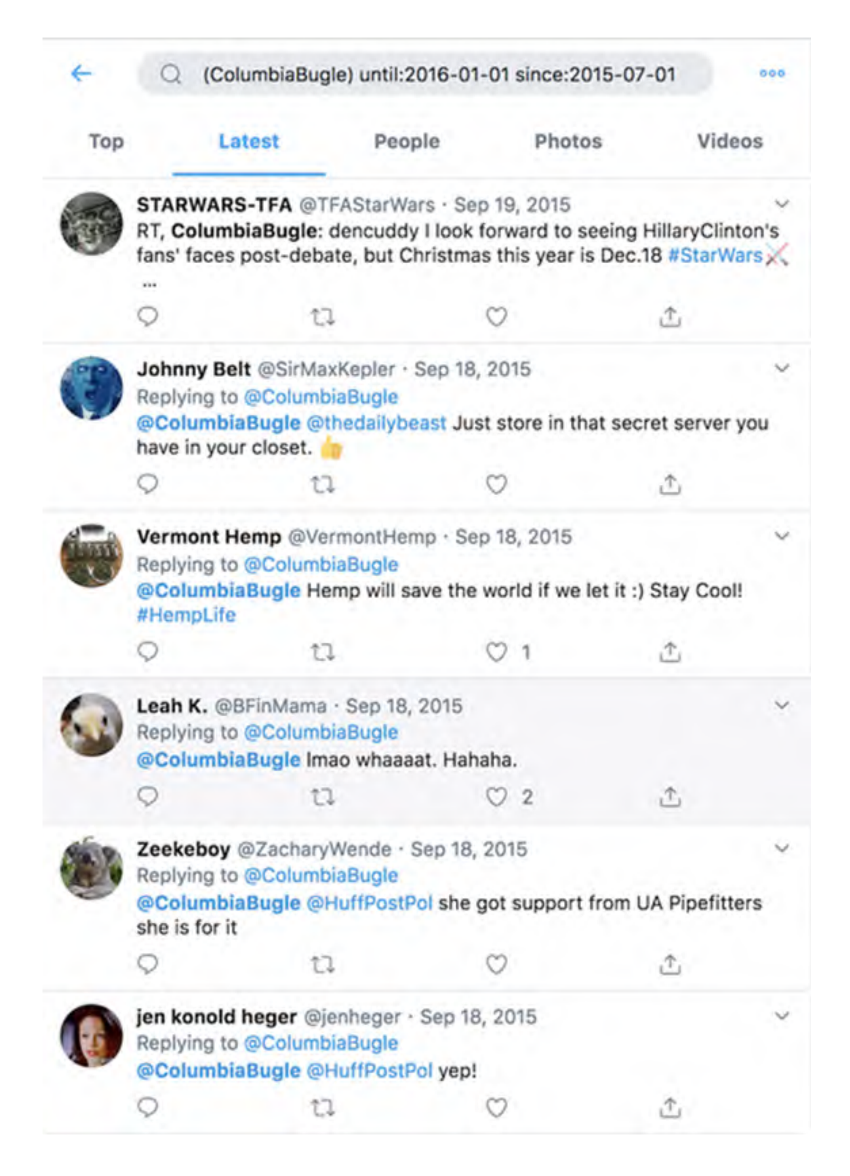
From
Month July | Day 1 | Year 2015

To
Month January | Day 1 | Year 2016

من المثير للانتباه هنا عدم وجود أي تغريدة في الحساب خلال الأشهر الستة الأولى من إنشائه.



قد يعني هذا ربما أن الشخص الذي يدير هذا الحساب قد حذف كافة التغريدات الأولى. ولأتأكد من ذلك وأقف عليه سيلزمني التعديل في طريقة بحثي، بأن أبحث عن تغريدات تذكر الحساب بدل البحث في تغريدات الحساب نفسه.

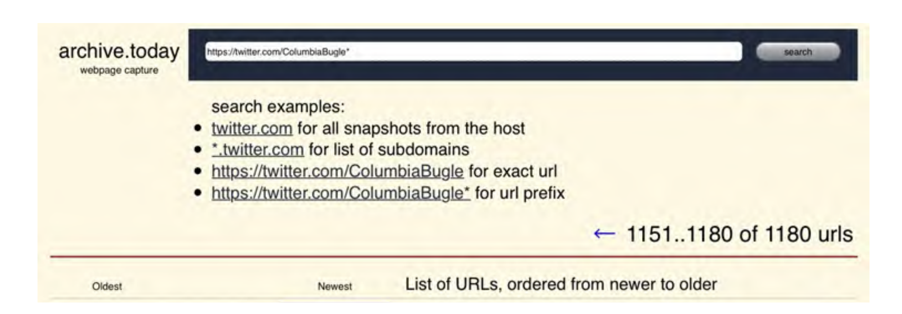


هذه الحوارات تثبت إذن أن حساب كولومبيا بيوغل قد حذف تغريداته التي نشرها في العام الأول من إنشاء الحساب، لكن السبب غير معروف،

والنظر إلى الحسابات الأولى التي تفاعل معها لا تُقدِّم لنا أيَّ خيوط لتفسير ما حصل.

للعثور على تغريدات محذوفة من فترة قصيرة، يمكن البحث في ذاكرة الكاش في جوجل (Cache)، ويمكن أحيانًا الاستفادة من ذلك للبحث عن تغريدات قديمة، وذلك في أرشيف الإنترنت (Wayback Machine)، أو غيرها من الأرشيفات الرقمية.

بالبحث في موقع الأرشيف Archive.is، تمكنت من العثور على عدد من التغريدات المحذوفة عن فعالية شارك فيها صاحب الحساب وقام فيها بعض طلبة الجامعة بكتابة عبارات مؤيدة لترمب. وللعثور على كافة التغريدات التي قد يكون شخص ما قد حفظها في الأرشيف، مثلما فعلت أنا للعثور على هذه التغريدة، يمكنك البحث عبر الرابط للحساب، مع وضع إشارة "النجمة *" بعد عنوان الحساب، على النحو التالي:





نـادرًا مـا يسـتطيع أي شـخص كان أن يفصـل بشـكل قاطـع مـا بيـن حياتـه الحقيقيـة وسـلوكه الرقمـي. فعلـى سـبيل المثـال، عملـت أنـا وزميلـي علـى [تقريـر صحفـي](#) حـول ادعـاء عـام 2016 بشـأن عمليـات تزويـر فـي الأصـوات، وهـو ادعـاء مضلـل ولاقـى انتشـارًا كبيـرًا علـى وسـائل التواصـل الاجتماعـي. وقـد حصلنـا فـي هـذا التقريـر علـى مسـاعدة من أحـد المعـارف فـي الحـيّ الـذي يقطـن فيـه صاحـب الحسـاب الـذي نشـر تغريـدة بالخبـر المضلل، وهو شخص ذو توجهات يمينية متطرفة.

ædonis | hotep
@lordaedonis
Follow

this is what I was talking about, they fixed it but it was on some nut shit at first.

RETWEETS 12,577
LIKES 9,686
7:46 am - 8 Nov 2016

ومع أن التغريدة بدأت على حساب معروف لدى المتابعين باسم المستخدم (@lordaedonis)، إلا أن الأشخاص المقربين منه في الحيّ الذي يقطن فيه كانوا يكتبون ردودًا على تغريداته باستخدام اسمه الحقيقي، والذي وضعناه في مقال "بروفايل" عن رائد أعمال مهووس بالشهرة تم الترويج لمقالته عبر حساب مدعوم من الكرملين، ما أتاح لها أن تصل إلى ملايين المستخدمين، ثم زاد في رواجها الشخص الذي كان في طريقه إلى الرئاسة الأميركية.



أفضل القصص الصحفية هي تلك التي تكشف عن الأشخاص الحقيقيين الذي يديرون حسابات مؤثرة بأسماء مستعارة على وسائل التواصل الاجتماعي. هذه الحسابات السرية لا تستسهل الاعتماد على الخوارزمية التي تعمل المنصة وفقها، وتكون أكثر حذرًا في بناء سلوكها كحالة هروب من الحياة العامة. إنها تتيح فرصة أداء دور المراقب والتواصل مع العائلة والأصدقاء بعيدًا عن حسابهم العام، أو التعبير عن الأفكار والآراء التي لا يرغب بالتعبير عنها باسمه الحقيقي لأسباب سياسية أو شخصية.

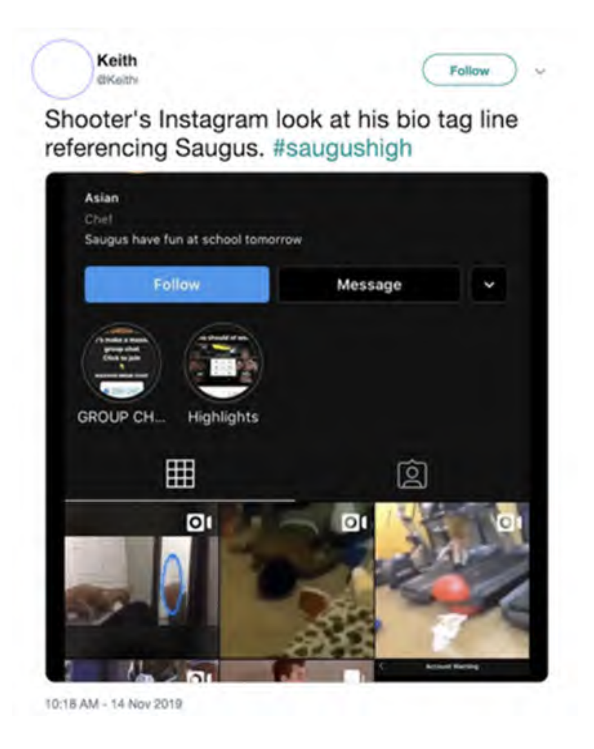
آشلي فاينبيرغ (Ashley Feinberg) صحفية رائدة في هذا المجال ومعروفة بالكشف عن مثل هذا النوع من القصص؛ فهي التي كشفت يومًا حقيقة حسابات تابعة لشخصيات بارزة، مثل جيمس كومي أو ميت رومني. لقد كانت وصفتها السحرية تتمثل في تتبع حسابات مغمورة لبعض الأفراد الذين قد يرغب كومي أو رومني بمتابعتها، لأنها تنتمي مثلًا لبعض أفراد عائلة كل منهما، ثم متابعة النبش في التغريدات القديمة إلى أن تجد حسابًا باسم مجهول، لكن المحتوى الذي ينشره وشبكة الأصدقاء والمتابعين فيه تماثل ما هو موجود في حساب آخر لأشخاص حقيقيين.

حذار من الحسابات المزيَّفة

لكل منصّة من المنصات سمة خاصة تعرف بها، وإمكانات معينة على مستوى الفائدة الصحفية وسهولة البحث والتصفح. لكن لا بدّ من توخي قدْر كبير من الحذر أثناء التعامل مع الحسابات على وسائل التواصل الاجتماعي، واتباع القاعدة الذهبية التي تقول: "ثق ولكن تحقَّقْ" (Trust but Verify).

ثمة جماعات من الناس يجدون متعة في خداع الصحفيين، وخاصة في المواقف المتعلقة بالأخبار العاجلة، ستجد الحسابات المزيفةُ فرصةً للظهور عبر نشر تغريدات سلبية أو تتضمن تهديدات أو معلومات مضلِّلة بهدف جذب اهتمام الصحفيين.

هذا الحساب المزيَّف على إنستغرام استخدم اسم الشخص المتورط في حادثة إطلاق نار في مدرسة ساوغوس في كاليفورنيا، علمًا أن الحساب قد أُنشئ بعد الحادثة. ومع ذلك فقد نجح صاحبه في لفت الاهتمام إليه عبر نشر صور على تويتر، إلى أن كشف موقع بازفيد نيوز لاحقًا أن الحساب لا علاقة له بالشخص الذي أطلق النار.



ولحماية نفسك من الوقوع ضحية هذا الشكل من التضليل والخداع، لا بدّ من التحقُّق من الحساب على وسائل التواصل الاجتماعي، عن طريق الشخص نفسه أو العائلة والأصدقاء أو الجهات الرسمية المعنية و/أو منصة التواصل الاجتماعي وقسم العلاقات العامة فيها.

أودّ أن أشير إلى نقطة أخيرة وربما تكون الأكثر أهمية في هذا النقاش، وهي التأكيد على أنه ليس ثمة ترتيب واحد صحيح للقيام بهذه الخطوات. كثيرًا ما أجد نفسي عالقة في عدة متاهات، وأمامي من صفحات الويب ما لا أستطيع حصره. لكن لا غنى عن اعتماد نظام محدّد يمكن استنساخه،

سواء عبر توثيق الخطوات التي اتبعتها في مستندات جوجل أم عبر الاستعانة بأداة مدفوعة مثل Hunchly من أجل المراقبة أثناء عملية البحث، من أجل توضيح الروابط بين الأشخاص ونمط سلوكهم الرقمي، والاستفادة من هذه النتائج في قصة صحفية مقنعة.

دراسة حالة 1: كيف كشفت عملية تحقق من حسابات على فيسبوك عن وجود شبكة بروباغندا منظمة في الفلبين؟

فيرنيس تانتوكو وغيما باغاياوا مندوزا

غيما باغاياوا مندوزا صحفية بخبرة تتجاوز 20 عامًا، وهي مديرة البحوث والإستراتيجيات في مؤسسة "رابلر"، وتترأس وحدة التحقق إضافة إلى الأبحاث التي تقوم بها المؤسسة في تعقب حملات المعلومات المضللة والزائفة.

فيرنيس تانتوكو هي عضو في فريق رابلر البحثي، وهي مختصة في عمليات التحقق ودراسة شبكات البروباغندا في الفلبين.

في خريف عام 2016 وصل مؤسسةَ رابلر رسالةٌ من محلل الاستثمارات جون فيكتورينو (John Victorino) تتضمن ما ادّعى أنها قائمة بـ 26 حسابًا مشبوهًا على فيسبوك في الفلبين.

بدأنا عملية التحقق والمراقبة لهذه الحسابات، وسرعان ما وجدنا أن التفاصيل المذكورة في الملفات الشخصية للحساب زائفة. وعلى مدى عدة أسابيع من التحقق، قادتنا هذه الحسابات إلى الكشف عن شبكة أكثر تعقيدًا من الصفحات والمجموعات والحسابات الأخرى.

قامت فيسبوك بحذف هذه الحسابات وعدد من الصفحات والمجموعات

المرتبطة بها. كما دفعتنا هذه العملية في رابلر إلى إنشاء أداة "Shark-tank" تساعد على مراقبة كيفية تدفق المعلومات إلى فيسبوك.

كما شجعتنا متابعةُ تلك القضية على العمل في سلسلة من قصص استقصائية أخرى ترصد عمليات البروباغندا والتضليل على فيسبوك وأثرها على الديمقراطية في الفلبين. وقد اشتملت هذه السلسلة على تحقيق يتعلق بأنشطة الحسابات الـ 26 المزيفة، ومن ثم استمرت التغطية لفهم الطريقة التي يجري بها استغلال منصة فيسبوك في الفلبين لغايات تتعلق بالتضليل السياسي وإيذاء الآخرين وتقويض الديمقراطية في البلاد.

توضح دراسةُ الحالةِ هذه طريقةَ عملنا في التحقق من الحسابات الـ 26 وكيف استفدنا من ذلك في الكشف عن شبكات تضليل أكبر.

التحقق من الهويات وكشف الحسابات الزائفة

كانت خطوتنا الأولى في التحقق من تلك المجموعة من الحسابات هي التأكد من أنها غير تابعة لأشخاص حقيقيين. وتطلّب هذا اللجوءَ إلى عمليات تحقُّق تقليدية مضمونة، فأنشأنا جداولَ لنضع فيها كافة التفاصيل المتعلقة بتلك الحسابات، بما في ذلك بيانات الملف الشخصي المذكورة، والصفحات التي يتابعونها وغيرها من المعلومات ذات العلاقة.

فمثلًا، لاحظنا أن المستخدمة صاحبة الحساب الذي يحمل اسم (Mutya Bautista) تصف نفسها بأنها "محللة برمجيات" في شبكة ABS-CBN، وهي أكبر شبكة تلفزة في الفلبين. وقد تحققت مؤسسة رابلر بدورها من ذلك عبر التواصل مع الشبكة، فكان الجواب بنفي وجود أي شخص بهذا الاسم بين موظفيها.



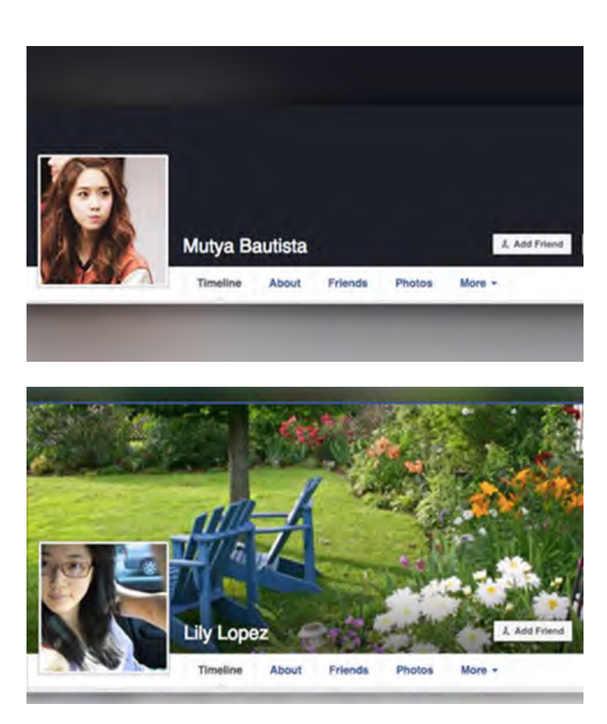
Personal Information	
Facebook ID	https://www.facebook.com/profile.php?id=10
Profile Name	Mutya Bautista
Occupation	Software Analyst
Current Company	ABS-CBN Corporation
Former Occupation 1	
Former Occupation 2	
Former Occupation 3	
Former Occupation 4	
Former Occupation 5	
Studied	Computer Engineering
Studied at	University of the Philippines
Went to	
Lives in	
Married to	
From	
Account Set-up Date	October 19, 2015

Liked Pages	Liked Pages Facebook ID
Okay Dito	https://www.facebook.com/vidtimestories/
The Philippine Pride	https://www.facebook.com/sirangplaka2/

Photos	Source of Photo
Profile Photo	Numerous sources. Im Yoona of SNSD
Cover Photo	

وعند استخدام أدوات البحث العكسي بالصور، تبين لنا أن العديد من الحسابات الـ 26 المشتبه بها قد استخدمت صور بروفايل لشخصيات مشهورة.

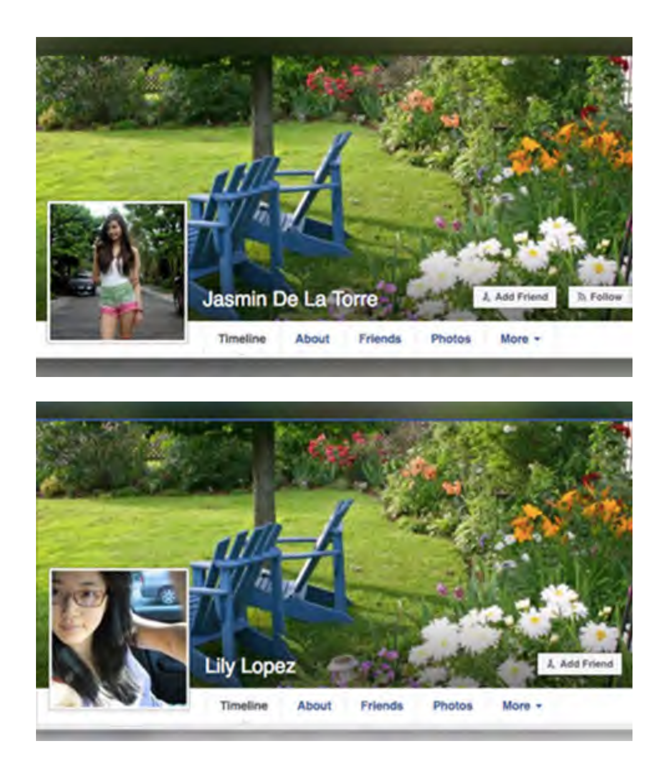
فحساب Bautista مثلًا استخدم صورة "Im Yoona"، وهي مغنية في فرقة "Girl's Generation" الكورية. وحساب "Lily Lopez" الذي يظهر أدناه قد استخدم صورة الممثلة الكورية "Kim Sa-rang".



أحد الحسابات باسم "Luvimin Cancio" استخدم صورة بروفايل عثرنا عليها في موقع إباحي، وقد اكتشفنا ذلك أثناء البحث عن الصورة بأداة البحث العكسي TinEye.



كما كان هنالك تشابه في صور الغلاف (Cover Photo) بين هذه الحسابات. نرى هنا مثلًا نفس صورة الغلاف في الحساب الذي يحمل اسم "Jasmin De La Torre"، وحساب "Lily Lopez".



ولاحظنا أيضا نمطًا مثيرًا للفضول في الحسابات الـ 26، وهو أن كافة هذه الحسابات لديها قائمة مجموعات أكبر من قوائم الأصدقاء. كان ذلك أمرًا يدعو للريبة؛ لأن معظم الناس في الفلبين لديهم عائلة وأصدقاء في الخارج، ومنصة فيسبوك عادة هي وسيلة يلجأ إليها الناس للبقاء على تواصل مع الآخرين، ولذلك نجد عادة قوائم طويلة من الأصدقاء على فيسبوك، وليس عددًا كبيرًا من المجموعات يفوق عدد الأصدقاء.

وجدنا في قائمة الأصدقاء لدى Bautista، والتي كانت متاحة للعامة أثناء عملية البحث التي قمنا بها، 17 حسابًا فقط، وكذلك الأمر في بقية الحسابات الـ 26 التي لم يتجاوز عدد الأصدقاء في كل منها 50 صديقًا، وذلك أثناء عملية التحقيق التي قمنا بها عام 2016.

في المقابل كانت Bautista عضوًا في أكثر من 100 مجموعة على فيسبوك، منها مجموعات مناصرة لفيرديناند ماركوس الابن، المرشح وقتها لمنصب نائب الرئيس، إضافة إلى عدد من المجتمعات لجاليات فلبينية في الخارج، ومجموعات أخرى للبيع والشراء، وكل مجموعة يتراوح عدد أعضائها بين عشرات الآلاف ومئات الآلاف، ويبلغ مجموع الأعضاء فيها جميعًا أكثر من 2.3 مليون عضوًا. فيما يلي قائمة ببعض أكبر هذه المجموعات، وأعداد الأعضاء فيها، إضافة إلى قائمة بالمنشورات التي نشرتها Bautista في هذه المجموعات.

GROUPS JOINED			CONTENT POSTED			
Group URL	Group Name	Group Members	DATE POSTED	Posts	Source	Group
https://www.facebook.com/groups/7551643712	Tambayan ng mga maranao samok 15	512,164		https://www.facebook.com/groups/321991	Okay Dito	We Support Bongbong Marcos
https://www.facebook.com/groups/bbmunited/	BongBong Marcos United	156,267	August 8, 2016	https://www.facebook.com/groups/166036	Okay Dito	OFW_KASABONG_KAIBIGAN GROUP
https://www.facebook.com/groups/5774321323	DOG LOVERS PHILIPPINES	133,437	August 5, 2016	https://www.facebook.com/groups/107711	Okay Dito	BABANGON AKO PARA SA PAGKAKAISA SOLID BONGBONG MARCOS GROUP (CAMANAVA AREA)
https://www.facebook.com/groups/OFWnewge	ON-LINE FILIPINO WORKER (OFW)	56,067	July 29, 2016	https://www.facebook.com/groups/166036	Okay Dito	OFW_KASABONG_KAIBIGAN GROUP
https://www.facebook.com/groups/6474477453	PINOY OFW SA UAE (Overseas Filipino W	53,169	July 29, 2016	https://www.facebook.com/groups/321991	Okay Dito	We Support Bongbong Marcos
https://www.facebook.com/groups/2042054097	Pinoy Networkers - Ads Center for Every	44,773	July 25, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/morefunphil	It's MORE FUN in the PHILIPPINES	44,339	July 24, 2016	https://www.facebook.com/groups/166036	Okay Dito	OFW_KASABONG_KAIBIGAN GROUP
https://www.facebook.com/groups/CAVITE SALE	CAVITE SALES,TRADE,SWAP motorcycle	42,147	July 24, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/pinoyofwsec	PINOY OFW'S MEETING SECTION	38,950	July 18, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/3481705587	Online Business For Filipinos Worldwide	38,202	July 17, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa United Kingdom	33,740	July 16, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/ofw.globalk	Ofw sa kuwait	33,569	June 25, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/entrepinoy/	PINOY AFFILIATE Marketing BUSINESS	33,199	June 16, 2016	https://www.facebook.com/groups/102468	Ask Philippine	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/3691104898	Pinoy Tambayan Ads Qatar	29,520	May 24, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/1505766333	Jobs hiring in lipa area/tanauan area/bat	28,212	May 18, 2016	https://www.facebook.com/groups/Bongbo	Okay Dito	SenaThorBongbongMarcosGroupPage_TeamKulit
https://www.facebook.com/groups/1458352404	Pinoy OFW in Malaysia..	26,076	May 17, 2016	https://www.facebook.com/groups/321991	Okay Dito	We Support Bongbong Marcos
https://www.facebook.com/groups/1921370942	Buy Sell Barter Philippines	25,888	May 17, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa China	25,128	May 17, 2016	https://www.facebook.com/groups/247154	Okay Dito	BONGBONG MARCOS FOR BETTER & GREATER PHILIPPINES 2016
https://www.facebook.com/groups/1619426761	TAMBAYAN NG MGA NAGHAHANAP NG T	24,387	May 16, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/swapphilipp	SWAP!!! PHILIPPINES	24,363	May 13, 2016	https://www.facebook.com/groups/1124		
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa Hong Kong	24,325	May 8, 2016	https://www.facebook.com/groups/1024		
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa Japan	23,803	May 7, 2016	https://www.facebook.com/groups/1196		
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa Spain	22,761	May 6, 2016	https://www.facebook.com/groups/1024		
https://www.facebook.com/groups/4823165519	SAMAHAN NG MAKUKULIT NA OFW 2	22,745	May 5, 2016	https://www.facebook.com/groups/1024		
https://www.facebook.com/groups/LDSEROPhili	LDS Employment Resource Center- Phili	22,711	May 5, 2016	https://www.facebook.com/groups/6812		
https://www.facebook.com/groups/sellsomethi	SELL SOMETHING PHILIPPINES	21,504	May 5, 2016	https://www.facebook.com/groups/3219		

Mutya Bautista
Timeline About Friends Photos More

وعبْر جمْع كافة هذه العناصر والبيانات المرتبطة بها، توصلنا إلى قناعة بأن كل هذه الحسابات مزيفة وتستخدم هويات مختلقة من أجل دعم أجندة أو بروباغندا ما.

شبكة مناصرة لماركوس

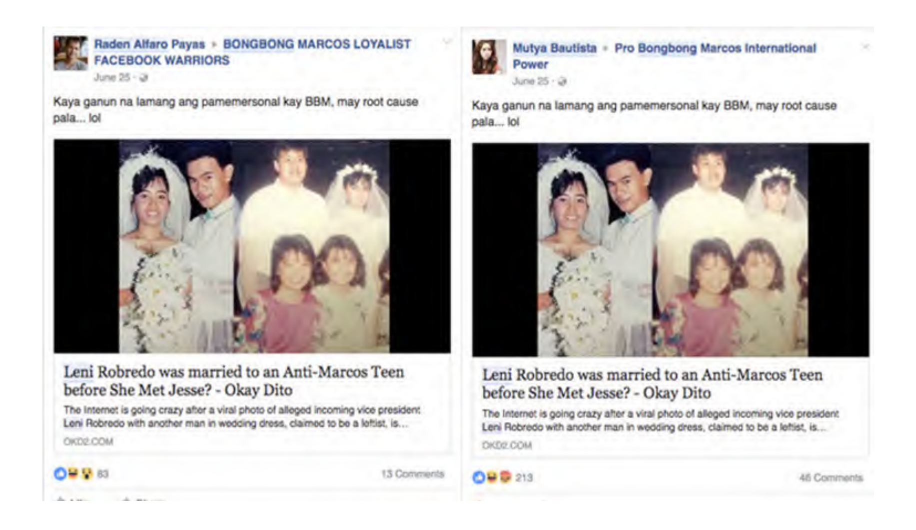
لاحظنا من خلال تتبع نشاط هذه الحسابات الـ 26 وتواريخ المنشورات المبكرة وأول صور بروفايل لها أنها قد أنشئت في الربع الأخير من العام 2015، إبان التحضير للانتخابات التي جرت في الفلبين في مايو 2016.

كما لاحظنا أن الحسابات نشطت في نشر محتوى ينكر الانتهاكات الموثّقة التي وقعت فترة الأحكام العرفية في سبعينات القرن الماضي في البلاد أثناء حكم الدكتاتور السابق ماركوس الأب. وقد ركزت الحسابات هجومها أيضًا على منافسي نجل ماركوس، فيرديناند "بونغ بونغ" ماركوس، والذي كان مرشحًا لمنصب نائب الرئيس.

في المثال الآتي نجد أن حساب Mutya Bautista قد نشر تقريرًا مفبركًا بخصوص منافِسة ماركوس الابن، ليني روبريدو التي فازت وقتها بمنصب نائب الرئيس. هذا الادّعاء الذي جرى دحضه لاحقًا يقول: إن ليني روبريدو كانت متزوجة في السابق من أحد الناشطين، قبل أن ترتبط بزوجها الحالي جيسي روبريدو الذي كان يشغل منصب وزير الداخلية والحكومة المحلية.

كان عنوان التقرير المذكور: "هل تزوجت ليني روبريدو مراهقًا معارضًا لماركوس قبل ارتباطها بجيسي؟"، وقد نشرته Bautista على مجموعة مناصرة لماركوس الابن اسمها (Pro Bongbong Marcos International Power)، مع تعليق يقول: "هذا يَكشف العداءَ الشخصي لماركوس الابن، هذا أصل الموضوع".

حساب مشبوه آخر باسم "Raden Alfaro Payas" نشر المقال نفسَه على مجموعة أخرى مناصرة لماركوس الابن اسمها (Bongbong Marcos loyalist Facebook warriors)، مع نفس التعليق السابق حرفًا بحرف وفاصلة بفاصلة، وفي اليوم ذاته.



عادة ما تُستخدم الحسابات الزائفة لنشر روابط داخل المجموعات، ويمكن أحيانًا اكتشاف ذلك عبر ملاحظة استخدام التعليق ذاته في المجموعات المختلفة.

أثناء هذا التحقيق كان من الممكن استخدام خاصية البحث البياني في فيسبوك (Facebook Graph)، من أجل البحث في منشورات عامة نشرها مستخدمون في مجموعات فيسبوكية. لكن فيسبوك قررت عام 2019 إيقاف العديد من خواص البحث المتقدم بما فيها خاصية البحث البياني. وعليه فإن الصحفي سيضطر حاليًا للبحث في المجموعات بشكل يدوي ليلاحظ أي أنماط معينة في المنشورات التي ينشرها المستخدمون.

مواقع مترابطة

عبر العمل على تحليل المحتوى الذي نشرته الحسابات المشبوهة

موضـوع التحقيـق لاحظْنـا كذلـك أنهـا جميعهـا كانـت تـروج مقـالات مـن مواقـع إلكترونيـة محـددة منهـا مثـلًا (OKD2.com)، وموقـع (askphilippines.com)، وموقـع why0why.com، وغيرها.

موقـع OKD2.com نشـر عـددًا مـن الأخبـار المفبركـة وغيرهـا مـن مـواد البروباغنـدا التـي تدافـع عـن أسـرة ماركـوس والرئيـس رودريغـو دوتيرتـي. حاليًا يظهـر الموقـع علـى أنّـه موقـع إعلانـات غيـر عـامّ، أمـا فـي سـبتمبر 2016 فقـد وجدنـا أن المحتـوى قـد نشـر 11،900 مـرة علـى فيسـبوك، وذلك عائد في جزء منه إلى نشاط الحسابات الزائفة التي حققنا بشأنها.

وعبـر تتبـع هـذه المواقـع الإلكترونيـة تمكنـت مؤسسـة رابلـر فـي نهايـة المطـاف مـن معرفـة مـن يقـف وراء الحسـابات الــ 26 الزائفـة، وهـو شـخص يدعى رادن ألفارو باياس (Raden Alfaro Payas).

تعقب مشغّلي الحسابات الزائفة

كعـادة العديـد مـن المواقـع التـي نراقبهـا فـي رابلـر، فـإن معلومـات تسـجيل النطـاق لموقـع OKD2.com غيـر متاحـة للعامـة. كمـا أن الموقـع لا يفصـح عـن الجهـة المالكـة للموقـع ولا عـن أسـماء مـن يكتبـون فيـه، ولا تجـد فيـه معلومات للتواصل، باستثناء نموذج على الموقع.

لكنـا تمكّنـا -لحسـن الحـظ- مـن اسـتخدام بيانـات النطـاق المؤرشـفة بشـكل أتـاح لنـا تحديـد شـخص لـه ارتبـاط بالموقـع، وذلـك عبـر أداة متوفـرة علـى domaintools.com.

لقد تبيـن لنـا أنـه فـي يوليـو 2015 كان موقـع OKD2.com مسـجلًا باسـم (Raden Payas) مـن سـكان مدينـة تانانـوان فـي باتانغـاس. كمـا وجدنـا أن الموقـع يشـترك فـي حسـاب "جوجـل أدسـنس" مـع مواقـع أخـرى، مثـل موقـع askphilippines.com، وموقـع why0why.com، وهـي مـن

المواقع التي كانت الحسابات الـ 26 تنشر المحتوى منها. وقد تمكنا من تحديد حساب "جوجل أدسنس" لهوية هذه المواقع عبر عرض رمز المصدر (Source Code)، للصفحات والبحث عن سلسلة من الأرقام التي بدأت بالرموز "ca-pub-". وبما أن كل حساب على "جوجل أدسنس" له رقم تعريف يبدأ بالرمز "ca-pub-"، وكل صفحة على الموقع مرتبطة بهذا الحساب؛ سيظهر عليها هذا الرقم التعريفي.

وإلى جانب المعلومات الخاصة باسم النطاق، فقد لاحظنا أن أحد الحسابات الـ 26 كان باسم "Raden Alfaro Payas (Unofficial)"، إضافة إلى وجود حساب آخر باسمه يحمل اسمَ المستخدم "realraden-payas"، ولاحظنا أنه تفاعلَ مع بعض الحسابات المزيفة.

فمثلًا كان هنالك تعليق على منشور من طرف "Luvimin Cancio" يشتمل على نفي للفظائع التي ارتُكبت خلال فترة الأحكام العرفية تحت حكم ماركوس الأب. وكان التعليق من حساب Payas "الحقيقي" أنه كان في الثانوية في سنوات الأحكام العرفية ولم يسمع قط عن تعرض أي شخص للقتل أو التعذيب.





Ferdinand B. Baga · Manila, Philippines
I like your piece. It's very good to enlighten the young generation of today. I was a teenager when Martial Law was declared in 1972. I haven't encountered any atrocities because Hindi ako pasaway. Only those who are involved in the underground movement had suffered but not all the people who are law abiding citizens. Malaya kami, wala kaming naranasan na policemen or soldiers' abuse. Maganda Ang martial law sa aming MGA kabataan, may discipline during that time!
Like · Reply · 9 · Sep 28, 2016 5:04pm



Raden Alfaro Payas · Carlos Hilado Memorial State College
Amen.... I was in highschool during Martial Law and I never heard someone in our barangay who was killed/tortured... Yong mga activists, kasalanan nila kung bakit sila sinaktan... activists noon , activists pa rin hanggang ngayon.. nothing's changed..
Like · Reply · 5 · Sep 28, 2016 6:06pm

انطلاقة مشروع "Sharktank"

هـذه الحسـابات الـ 26 المزيفـة ومقـدار تأثيرهـا ووصولهـا دفـع مؤسسـة رابلـر إلـى إنشـاء قاعـدة بيانـات "Sharktank" لأجـل أتمتـة عمليـة جمـع البيانات من المجموعات والصفحات العامة على فيسبوك.

ومنـذ أغسـطس 2019، تعقبـت رابلـر حوالـي 40 ألـف صفحـة بملاييـن المتابعين.

وهكذا فـإن مـا بـدأ كعمليـة تحقـق واسـتقصاء بشـأن مجموعـة مـن الحسـابات المشـبوهة تحـوَّل إلـى عمليـة تعقُّـب مسـتدامة لشـبكة مـن آلاف الحسـابات الوهميـة والحقيقيـة، والمجموعـات الفيسـبوكية والصفحـات، والتـي تنشـر المعلومات المضلِّلة والبروباغندا وحملات التشويه وتقويض الديمقراطية.

دراسة حالة 2: كيف اكتشفنا أن أكبر صفحة خاصة بحراك "حياة السود مهمّة" مزيفة؟

دوني أوسوليفان

دونـي أوسـوليفان هـو مراسـل يعمـل مـع شـبكة سـي إن إن، ومهتـم بمسـألة التداخـل بيـن التكنولوجيـا والسياسـة، وهـو عضـو فـي فريـق "سـي إن إن بزنـس" ويعمـل عن كثـب مع وحدة التحقيقات الاسـتقصائية فـي الشـبكة لتعقـب وكشـف حمـلات التضليـل التـي تسـتهدف الناخبيـن الأمريكيين.

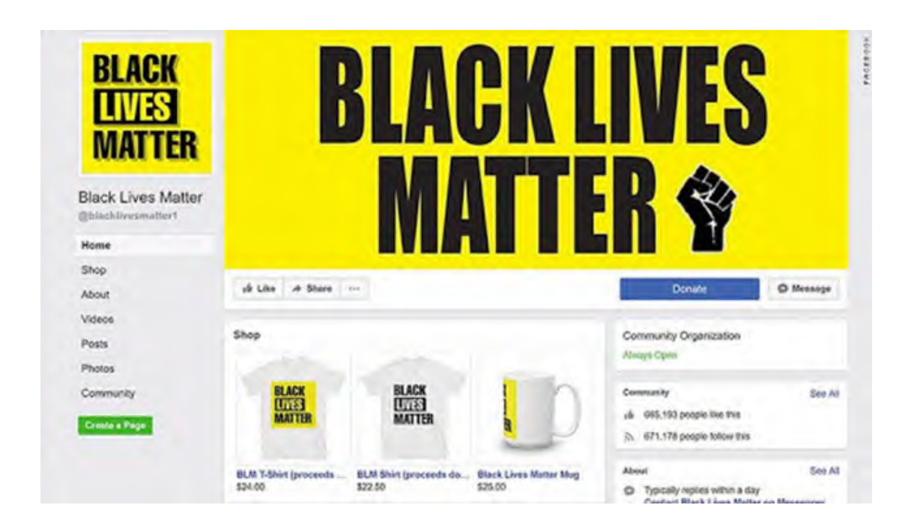
فـي صيـف وخريـف عـام 2017، وحيـن بـدأ العالـم يتعـرف علـى المزيـد من التفاصيـل بشـأن المسـاعي الروسـية الهائلـة للتأثيـر علـى رأي الناخبيـن الأمريكييـن عبـر وسـائل التواصـل الاجتماعـي، اتّضـح أن الأمريكييـن مـن أصـول أفريقيـة وحَـراك "حيـاة السـود مهمـة" كانـوا واحـدًا مـن أهـم أهـداف حملة الكرملين لخلق الانقسامات والتشويش على الآراء.

وقـد قضينـا أنـا وزملائـي فـي شـبكة "سـي إن إن" عـدة أشـهر فـي إعـداد تقاريـر تكشـف دور روسـيا فـي تحريـك مجموعـة مـن أكبـر الحسـابات المحسـوبة علـى حـراك "حيـاة السـود مهمـة" علـى وسـائل التواصـل الاجتماعـي. وكثيـرًا مـا تلقيتُ أثنـاء الحديـث مـع ناشـطين فـي هـذا الحـراك أسـئلةً مـن قبيـل: "هـل تعـرف مـن يديـر الصفحـة الأكبـر لحـراك "حيـاة السود مهمة" على فيسبوك؟".

الأمـر المفاجـئ هـو أنـه لـم يكـن أحـد يعـرف الجـواب، حتـى أبـرز الناشـطين في الحـراك والفاعليـن فـي الميدان بينهـم. بعضهـم أثـار شـكوكًا عامـة بـأن الصفحـة

قد تكون تدار من روسيا. لكن التحقيق الذي أجريناه أثبت أن الصفحة لم تكن تدار من روسيا ولا أميركا، بل من طرف رجل أبيض في أستراليا.

الصفحة باسم "Black Lives Matter" لا تثير أي شبهة. كان يتابعها حتى أبريل 2018 حوالي 700 ألف متابع. حرصَت الصفحة على مشاركة روابط لتقارير صحفية تتحدث عن عنف الشرطة والتمييز ضد السود، وكانت تدير حملات لجمع التبرعات على الإنترنت، بل وكان لها أيضًا متجر إلكتروني يبيع منتجات خاصة بحراك "حياة السود مهمة".



ليس من النادر وجود صفحة بهذا الحجم ولا يُعرف من يديرها. فبعض الناشطين لا يرغبون في أن تكون صفحة ما مرتبطةً بهم بشكل شخصي؛ وذلك لتجنب حملات الإساءة الشخصية الموجهة ضدهم، أو تفادي لفت انتباه الأجهزة الأمنية إليهم، وهي تبحث عن أي ثغرة لمنع المظاهرات.

ففي أماكن أخرى خارج الولايات المتحدة، كانت الإمكانية المتاحة للناشطين بإدارة الصفحات دون نسبتها إليهم عنصرًا بالغ الأهمية في النشاط الحقوقي الرقميّ، وأمرًا أساسيًا في نجاح تأثير بعض الحَراكات. (وقد كان ذلك تحديدًا ما استغلّته روسيا، ما أثار الشكّ باحتمال أن تكون هذه الصفحة الخاصة بحقوق السود تُدار من طرفها).

وحين بدأتُ الاهتمامَ بشكل أكبر بشأن هذه الصفحة الغامضة، قدَّم لي جيريمي ماسلر -وهو محقق حرّ يمتلك براعة مذهلة في التنقيب الرقمي- مساعدةً مهمة. لقد بحث ماسلر عن بيانات تسجيل النطاق (Domain Registration) للمواقع الإلكترونية التي كانت هذه الصفحة الضخمة تنشر روابطها باستمرار. ورغم أن هذه البيانات لم تكن متاحة للعامة، إلا أنه اكتشف أن أحد هذه المواقع، ولفترة قصيرة من العام 2016، كان مسجلًا باسم شخص يعيش في مدينة بيرث في أستراليا، وهو رجل أبيض يدعى إيان ماكاي.

```
Domain Name: BLACKLIVESMATTERWEBSITE.COM
Registry Domain ID: 2065833077_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.launchpad.com
Registrar URL: LaunchPad.com
Updated Date: 2018-10-13T08:00:42Z
Creation Date: 2016-10-13T07:10:33Z
Registrar Registration Expiration Date: 2018-10-13T07:10:33Z
Registrar: Launchpad, Inc. (HostGator)
Registrar IANA ID: 955
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: ian mackay
Registrant Organization: Website
Registrant Street:
Registrant City: brisbane
Registrant State/Province: Queensland
Registrant
Registrant
Registrant
Registrant
Registrant
Registrant Fax Ext:
Registrant Email: blacklivesmatter1@hotmail.com
```

تواصل ماسلر مع ماكاي، وأخبره الأخير بأنه يشتري أسماء النطاقات ويبيعها كهواية جانبية، وأنه لا علاقة له بالصفحة على فيسبوك. وقد كان ذلك هو الجواب نفسه الذي تلقيته من ماكاي حين تواصلت معه عبر الهاتف بعد عدة أشهر، وكنا حينها قد اكتشفنا أن ماكاي هذا قد سجّل عشرات أسماء النطاقات الإلكترونية، وعدد غير قليل منها يتعلق بحراك السود.

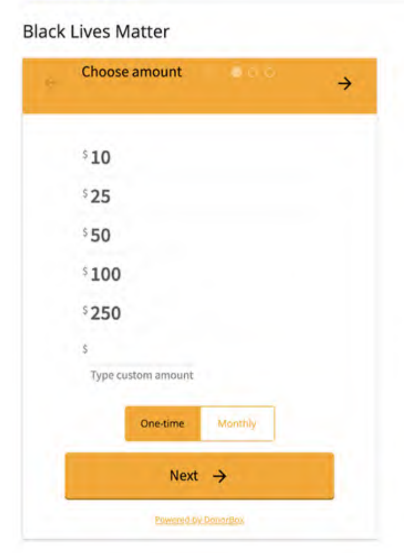
وبالرغم من التوجس بشأن الصفحة، وما سمعته من العديد من الناشطين بأنهم يشكّون في أمرها، إلا أنني لم أستطع الجزم بعدم صحّة ادعاء ماكاي بشأن أسماء النطاقات المسجلة باسمه؛ فأسماء النطاقات قد تكون مصدر دخل جيد، والناس يشترون أسماء النطاقات ويبيعونها بشكل مستمر، ولاسيما أن ماكاي هذا قد اشترى وباع العديد من أسماء

النطاقات الأخرى غير المرتبطة بحراك السود.

لكن أمرًا مريبًا قد حصل، وأثار الشكّ من جديد. فبعد دقائق معدودة من اتصالي بماكاي، تم إزالة الصفحة عن فيسبوك. لم يكن ذلك إجراءً من طرف إدارة الموقع، بل كان أمرًا قام به من يدير الصفحة، والذي لم يحذفها تمامًا، وإنما أزالها بشكل مؤقت، وهذا ما دفعني أنا وماسلر للبحث بشكل أعمق.

صفحة الفيسبوك موضوع التحقيق والتي فُعّلت من جديد في الأسابيع التي تلت مكالمتي مع ماكاي، كانت قد أطلقَت عدةَ حملات لجمع التبرعات، تدّعي أنها لأهداف تخدم حراك "حياة السود مهمّة". وادّعت الصفحة في إحدى هذه المرات أنها تجمع تبرعات للناشطين في مدينة ممفيس في ولاية تينيسي. فتواصلت مع بعض الناشطين هناك، وتبين أن أحدًا لا يعرف أي شيء عن الحملة، ولا عن النقود التي جمعت، ولا أين ذهبت. بل إن ناشطين آخرين أخبرونا بأنهم شكّوا في الأمر باعتباره تحايلًا، وقاموا بالتبليغ عن الصفحة، لكن إدارة فيسبوك لم تتخذ أي إجراء.





Thank you for taking a look at this page, We appreciate all donations and all proceeds go toward Black Lives Matter Media campaigns which is an amazing cause aimed at bringing media attention to Racism and Bigotry. We are not sponsored or funded by any other part of the BLM movement or big companies or celebrities and we soley rely on the kindness of every day supporters like you. So far we have posted over 30 000 news stories and had literally millions of visits to the website www.blacklivesmatter1.com , grown our Facebook page to over 360 000 supporters www.facebook.com/blacklivesmatter1and we have a reach of up to 8 million people a week who see the most confronting stories of injustice to Black people. We want to reach even more people so our children might not have to suffer racism in the way we do now in the future. This movement was formed by the people and is being moved forward by the people. We have largely funded this ourselves and we are a very, very small crew. It is becoming a struggle to keep going so we have decided to see if people are willing to get behind us and help. We understand a lot of people are doing it tough, if you are you can still help by sharing this page to others. Thank you so much!



عندها شرعتُ بالتواصل مع عدد من منصات الدفع الإلكتروني وجمْع التبرعات التي تعاونَت معها الصفحة في حمَلاتها، بدأت هذه الشركات بإيقاف الحملات، وذكرت أن ذلك بسبب الإخلال ببعض القواعد الإجرائية التي تشترطها. لم تُفصح أيٌّ من هذه المنصات عن أي معلومات بشأن الحساب الذي كانت تُحوَّل إليه هذه التبرعاتُ، متذرّعةً بحق المستخدم في الخصوصية، وهو الأمر الذي يفرض تحديًا كبيرًا في هذا النوع من التحقيقات، والتي تمنع المنصات ومقدمي الخدمات الرقمية في معظم الحالات من الكشف عن هوية أو معلومات الاتصال الخاصة بأصحاب الحسابات.

اتضح لي لاحقًا عبر مصدر مطلع على بعض الدفعات التي تمت معالجتها بأن حسابًا واحدًا على الأقل كان مرتبطًا بحساب بنكي وعنوان بروتوكول أستراليين. كما أخبرني مصدر آخر أن مجموع التبرعات قد بلغ حوالي 100 ألف دولار أمريكي. وهنا تجدر الإشارة إلى أهمية بناء شبكة مصادر من العاملين في الشركات التقنية والذين يكونون على استعداد لتقديم معلومات تُحجم الشركات عن تقديمها بشكل رسمي، وهذا أمر بالغ الأهمية؛ نظرًا إلى أن العديد من التحقيقات الصحفية لا يمكن أن تصل إلى نتيجة مفيدة في حال الاعتماد بشكل حصري على المعلومات المتاحة في المصادر المفتوحة، وذلك لأن الأطراف المنخرطين في أنشطة احتيال أو تضليل يطوّرون أساليبهم بشكل مستمر.

قدّمتُ هذه المعلومات التي توصلت إليها إلى إدارة فيسبوك، وطلبت منهم التعليق على القصة، وأخبرتهم بأني أمتلك أدلة تفيد بأن الصفحة مرتبطة بأستراليا، وأن شركات الدفع الإلكتروني قد أوقفت حملات التبرع بعد التحقق من الأمر، وأننا اكتشفنا أن بعض التبرعات قد ذهبت بالفعل إلى حساب بنكي في أستراليا. لكن المتحدث باسم فيسبوك قال: إن المنصة أجرت تحقيقاتها، وتأكدت من عدم حصول "أي سلوك ينتهك معايير المجتمع في منصتنا".

لكن حين قمنا بنشر التحقيق، أبلغت مسؤولًا أكبر في فيسبوك بشأن

تحفّظاتـي حـول التحقيـق الـذي قامـت بـه المنصـة، وردِّ المتحـدث الرسـمي علـيّ بشـأن القضيـة، وكان ذلـك كفيـلًا بدفـع المنصّـة إلـى التحـرّك وحـذف الصفحة.

كمـا قـام اتحـاد العمـال فـي أسـتراليا، حيـث يعمـل مـاكاي، بإطـلاق تحقيـق خـاص بـه عقـب انتشـار تحقيـق سـي إن إن، وفـي غضـون أسـبوع فقـط قـام الاتحـاد بفصـل مـاكاي مـن عملـه، إضافـة إلـى مسـؤول آخـر أفـاد الاتحـاد بأنه منخرط في الفضيحة.

لعـل أحـد أهـم الجوانـب التـي يجـدر الالتفـات إليهـا فـي هـذه الحالـة هـو نطـاق الأسـاليب التـي اعتمدنـا عليهـا أنـا وماسـلر مـن أجـل الوصـول إلـى النتيجـة المرجـوّة. لقـد اعتمدنـا بشـكل كبيـر علـى مواقـع الأرشـيف الرقمـي مثـل "Wayback Machine"، والتـي أتاحـت لنـا التعـرف علـى شـكل المواقـع الإلكترونيـة التـي كانـت الصفحـة تنشـر روابطهـا، إضافـة إلـى الصفحـة نفسها قبل أن نشكّ في أمرها.

وقـد حققنـا فائـدة كبيـرة مـن هـذه العمليـة، وذلـك لأنـه بعـد التواصـل الأولـي الـذي أجـراه ماسـلر مـع مـاكاي بـدأ المسـؤولون عـن الصفحـة بمحاولـة طمس أي آثار محتملة تدل عليهم.

كمـا اسـتخدمنا الخدمـات التـي تتيـح تعقـب عمليـات تسـجيل أسـماء النطاقـات، مثـل موقـع DomainTools.com، وذلـك مـن أجـل التحقـق مـن المواقـع التـي سـجلها مـاكاي، والعثـور علـى معلومـات الاتصـال الخاصـة بـه. وقـد اعتمـد ماسـلر بشـكل مكثـف علـى أداة البحـث البيانـي فـي فيسـبوك (Face-book Graph Search)، قبـل أن تقـوم الشـركة بإلغائهـا، وذلـك فـي عمليـة تعقـب حسـابات فيسـبوك الوهميـة التـي تـم إنشـاؤها مـن أجـل الترويـج للصفحة موضوع التحقيق في مجموعات فيسبوكية.

بقـي أخيـرًا أن نشـير إلـى أن أدوات التحقـق مـن المعلومـات والبيانـات عبـر المصـادر المفتوحـة إضافـة إلـى أدوات البحـث المتوفـرة عبـر الإنترنـت كتلـك

التي أشرنا إليها آنفًا للوصول إلى بيانات خاصة بأسماء النطاقات، هي أدوات بالغة الأهمية، لكن لا يمكن للصحفي الاكتفاء بها.

فالتواصل الهاتفي مع ماكاي، وبناء شبكة من المصادر التي ساعدت في توفير بعض المعلومات الحصرية التي كان يصعب الحصول عليها بشكل رسمي، هي أساليب صحفية تقليدية، وقد كان لها دور أساسي في الكشف عن عملية الاحتيال التي حصلت.

الفصل الثاني: العثور على المريض رقم صفر

هينك فان إيس

يشغل هينك فان إيس منصب مقيّم في شبكة بوينتر الدولية للتحقق (Poynter International Fact-Checking Network)، ويتمثل اهتمامه الرئيسي بالعثور على قصص صحفية عبر دراسة البيانات. يقدم هينك دورات تدريبية للمهنيين في مجال البحث عبر الإنترنت، ووسائل التواصل الاجتماعي، والوسائط المتعددة، ويقدّم خدمات التدريب للعديد من المؤسسات العالمية، مثل شبكة إن بي سي، وباز فيد نيوز، وآي تي في، وغلوبال ويتنس، ومؤسسة إس آر إف، وأكسل سبرينغر، والعديد من المنظمات والجامعات. لدى هينك موقعان إلكترونيان هما whopostedwhat.com، وموقع graph.tips، ويستخدمها الصحفيون باستمرار للتحقق عبر وسائل التواصل الاجتماعي. ويمكن متابعة هينك على تويتر على @henkvaness.

على مدى عدة عقود، عُرف مضيف الطيران الكندي غيتا دوغا (Gaëtan Dugas) بوصف "المريض رقم صفر"، إذ يوصف بأنه الشخص الأول الذي أدخل عدوى الإيدز إلى الولايات المتحدة الأمريكية.

هذا الوصف الذي تكرر حتى تكرّس في الكتب والأفلام وعدد لا يحصى من التقارير الإخبارية والصحفية، جعله ببساطة "الشرير الأفظع" الذي نقل الوباء الذي سيتسبب لاحقًا بمقتل أكثر من 700 ألف شخص في أمريكا الشمالية.

لكن في الحقيقة كان الواقع بخلاف ذلك. ما حصل هو أن بيل دارو، أحد المسؤولين العاملين مع هيئة المراكز الأمريكية لمكافحة الأمراض والوقاية منها (CDCP) قد فحص دوغا هذا، وكتب على تقريره عبارة "Patient O"، بمعنى "المريض المسافر من كاليفورنيا" (Out-of-Cal-ifornia)، لكن بقراءة خاطئة للحرف "O" على أنه "0"، أي صفر، انطلقت موجة عارمة من ردود الفعل التي نما حولها حجم ضخم من المعلومات المغلوطة التي ما يزال الناس يتناقلونها حتى وقت قريب.

فمن الوارد إذن -حتى للصحفيّ- أن يركّز اهتمامه على الشخص الخاطئ إن لم يكن يمتلك كفاءة عالية في البحث والتحقق. في هذا الفصل سنتعلم كيفية الوصول إلى المصادر الأولية على الإنترنت، وتفادي النتائج السطحية عبر النبش المعمّق في الشبكة.

1. المخاطر المرتبطة بالاستعانة بالمصادر الأولية وكيفية معالجتها

يحب الصحفيون المصادر الأولية (Primary Sources) على الإنترنت، وذلك لأن الأدلة الأولى قد تكون عادة في مقال صحفي أو دراسة علمية أو بيان صحفي أو على حساب على وسائل التواصل الاجتماعي أو أي مصدر آخر محتمل على الإنترنت.

لكن القيام بعملية بحث باستخدام الكلمات الرئيسية المطلوبة على موقع حكومي سيعطيك انطباعًا بأن ما يظهر في نتائج البحث هو ما يتوفر بالفعل لديهم. إلا أن الأمر بخلاف ذلك في كثير من الأحيان. لندرس معًا هذا المثال، ونذهب إلى هيئة الأوراق المالية والبورصات الأمريكية، وهي المصدر الذي يستخدم عادة للحصول على معلومات مالية عن أي مواطن أمريكي أو حتى عن رجال أو سيدات أعمال في مختلف أنحاء العالم. ولنقل مثلًا أننا نريد تحديد المرّة الأولى التي وردت فيها عبارة "Dutch Police" (الشرطة الهولندية) على موقع الهيئة، ويمكن

الاستعانة بمحرك البحث المدمج في الموقع للقيام بذلك:



ستحصل في عملية البحث هذه على نتيجة واحدة، وهي وثيقة تعود للعام 2016، وقد نستنتج أن هذا بالفعل هو كل ما يمكننا أن نحصل عليه، هل هذا صحيح؟

And I have cooperated with the FBI in the pump and dump scam. The Dutch police. The same thing, with the Scotland Yard over the years. And I certainly understand fraud and fraudulent activities.

كلّا. الذكرُ الأول لهذه العبارة في موقع الهيئة كان في العام 2004، أي قبل 12 عامًا من تاريخ النتيجة التي حصلنا عليها أول مرة، وذلك في بريد تم رفع صفة السريّة عنه ولكنه مشفَّر.

The increase was primarily the result of several large international contract awards, such as the Dutch Police, an Australian utilities company and a Russian utilities company, and additional orders received for Z/I Imaging Digital Mapping Cameras.

لن تعثر على هذه النتيجة من خلال شريط البحث على موقع الهيئة، رغم أنّي قد حصلت على هذه المعلومة أعلاه عبر الموقع نفسه. فما الذي حصل؟

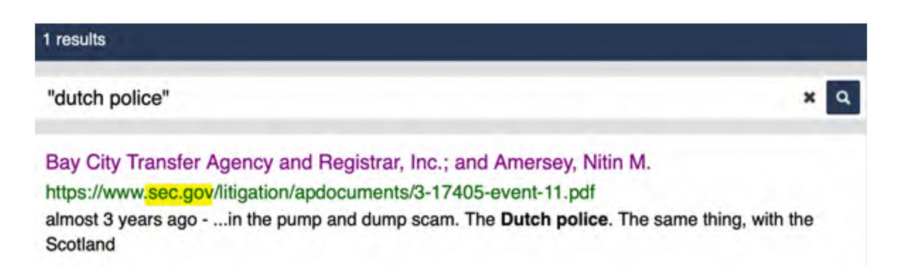
عليك مبدئيًا أن تمتلك بعض الشكّ الصحّي بمحركات البحث من المصادر الأولية، وذلك لأنك لن تحصل منها سوى على انطباع خاطئ عن المحتوى الفعلي الذي يتضمنه الموقع وقواعد البيانات التي يرتبط بها.

إنّ الطريقة المثلى للبحث تتمثل أولًا بالقيام بعملية "التحقق من المصدر الأولي".

التحقق من المصدر الأولي

الخطوة 1: النظر في الرابط غير الفعال

عملية البحث الأُولى في موقع الهيئة كشف لنا عن نتيجة واحدة فقط:



فلنحاول أن نستغل هذه الخيبة البحثية. أولًا، قم بحذف المقطع (https://www.) من الرابط، ثم ابحث عن أول شرطة مائلة للخلف (backslash) في الرابط المتبقي، وهي في هذا المثال قبل الكلمة litigation، والجزء الذي قبلها هو ما نحتاج إليه، وهو في حالتنا هذه (sec.gov).

الخطوة 2: استخدام كلمة "site"

اذهب إلى محرك بحث عام، وابدأ البحث بكتابة ("Dutch police") بهذا الشكل، ثم اكتب كلمة (site)، يتبعها مباشرة الرابط الذي حصلنا عليه (بدون مسافات). بهذه الطريقة يمكنك أن تعرف ما إذا كان المصدر الأصلي الذي بحثت فيه يوفر لك كل النتائج بالفعل أم أنه يتضمن نتائج أخرى:



"dutch police" site:sec.gov

البحث عن ملفات محددة

يمكنك الآن الاستعانة بهذه الطريقة للبحث في المصادر الأولية بما يناسب ما تبحث عنه. فلنذهب مثلًا إلى قسم البيانات الصحفية في الموقع الإلكتروني لمحاكم ولاية نيوجيرسي. فلنفترض مثلًا أنك تريد البحث عن وقت قيام نقابة المحامين في مقاطعة ميرسر (Mercer County) بالمطالبة بوجود برنامج خاص يُدعى "يوم القانون" (Law Day). لو بحثت في قسم البيانات الصحفية فلن تجد أي نتيجة تدل على المطلوب، ولن يظهر لديك أي بيان بعنوان يشتمل على عبارة (Mercer County Bar Association).

Filter by Published Date back to 1999

November 2018 to November 2019 Apply

Filter by Title:

الآن انظر إلى رابط تلك الصفحة المملوء بالبيانات الصحفية غير المدرجة بطريقة مرتبة:

njcourts.gov/public/pr.html

يظهر أن المواد الخاصة بالعلاقات العامة مخفية في ملف (/public)، وهذا ما يجب أن تستخدمه في عملية البحث على جوجل:

"mercer county bar association" site:njcourts.gov/public/

وهكذا ستعثر على مرادك:

About 6 results (0,31 seconds)

New Jersey Judiciary Law Day - NJ Courts

https://www.njcourts.gov › public › lawday › lawday2018 ▾

May 1, 2018, 10:00 AM, Richard J. Hughes Justice Complex, Trenton, Law Day Program a
Naturalization Ceremony, General Public, Yes, open to the public.

توقع الملفات

لدى الصين وزارة خاصة بالبيئة والمناخ، وقد يحتاج الصحفي مثلًا إلى معرفة ما إذا كان موقع الوزارة الإلكتروني يشتمل على وثائق باللغة الإنجليزية عن الشركة الألمانية سيمنز. باتباع الوصفة التالية، ستعثر على وثائق باللغتين الصينية والإنجليزية في نتائج البحث:



ولو كنت تريد الاطلاع على الوثائق الإنجليزية فقط، فربما سيفيد أن نستخدم كلمة English مع الرابط. وبالفعل، سنجد النتائج التالية:



2. تتبع مسار الوثائق

أحيانًا لا تكون المعلومات التي نبحث عنها موجودة على صفحة ويب، ولكنها موجودة في وثيقة مرفوعة على الموقع الإلكتروني. بهذه الطريقة الآتية سيكون بإمكانك تتبع مسار وثيقة ما عبْر استخدام صيغ البحث المتقدم.



روس ماكتريك هو أستاذ مشارك في قسم الاقتصاد في جامعة غويلف في أونتاريو. في العام 2014 قدم عرضًا أمام مجموعة من الناس غير المقتنعين بمخاطر التغير المناخي. فلنحاول معًا العثور على الدعوة الخاصة بذلك اللقاء. نحن نعرف مبدئيًا أن المحاضرة عقدت في 13 مايو، 2014، وكانت الفعالية الحادية عشرة ضمن فعالية غداء العمل السنوي (Annual Luncheon) من تنظيم جمعية "أصدقاء العلوم" (Friends of Science). لو بحثنا في جوجل باستخدام هذه العبارات، فإننا لن نعثر على أي نتيجة:

No results found for **"Friends of Science 11th Annual Luncheon 2014" "invitation"**.

السبب هو أن كلمة "invitation" لا ترد في العديد من بطاقات الدعوة؛ لأنها بطاقة يُعرف اسمها من محتواها؛ تمامًا كالخريطة، والتي لا تجد كلمة "خريطة" مكتوبة عليها في كثير من الحالات. فما العمل؟

الخطوة الأولى: حدد نوع الوثيقة

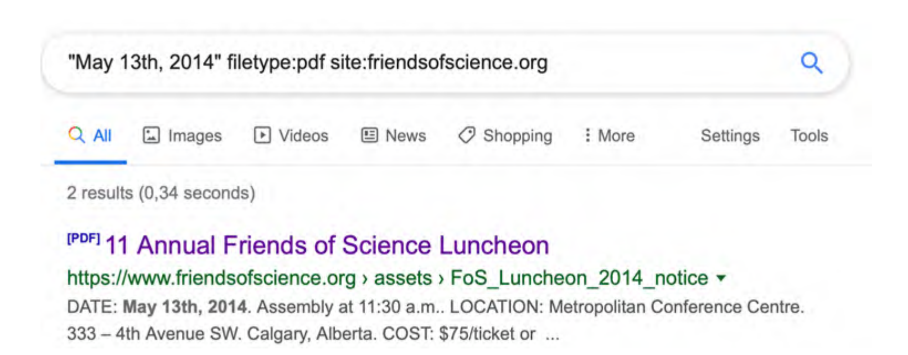
حاول أن تحدد العنصر المشترَك بين الدعوات التي تُرسل عبر الإنترنت. عادة ما تكون الدعوة بصيغة PDF. يمكن أن تبحث عنها عبر استخدام صيغة "Filetype:pdf"، ويمكن أن تجدها.

الخطوة الثانية: ابحث باستخدام العناصر التي تثق بصحتها

قد يصعب عليك تحديد العبارة التي صيغت بها الدعوة، لكن ما تعرفه بالتحديد بشأن الفعالية، عبر الفيديو المتوفر على يوتيوب، هو أنها كانت في 13 مايو، 2014، وقد يكون من الوارد جدًّا أن التاريخ مذكور في نص الدعوة. (تأكد عند البحث من استخدام الصيغ المختلفة لكتابة التاريخ: May 13 أو May 13th) إن كنت تبحث بالإنجليزية.

الخطوة الثالثة: من هي الأطراف المعنية؟

نحن نعرف أن الجهة المنظِّمة هي جمعيةُ "Friends of Science"، وموقعهم الإلكتروني هو friendsofscience.org. حين تدمج بين هذه الخطوات الثلاثة، فإن النتيجة على جوجل ستكون كالتالي:



وهكذا نكون قد وجدنا الدعوة إلى الفعالية في النتيجة الأولى في محرك البحث.





كثيرًا ما يتم الإشارة إلى جمعية "أصدقاء العلوم" ومقرُّها في كالغاري على أنها مجموعة تشكّك في مخاطر التغير المناخي، وأنها تحصل على جزء من تمويلها من شركات تعمل في قطاع الغاز والنفط. فكيف يمكن أن نبحث عبر الإنترنت لمعرفة المزيد عن الجمعية وشبكة داعميها ومموليها؟

الخطوة 1: كن أكثر تحديدًا

ستعثر غالبًا على عدد هائل من النتائج لو اكتفيت بالبحث عن "Friends of Science"، لذلك ينصح بأن تضيف المكان، كالغاري (Calgary) إلى البحث.

الخطوة 2: حدّد نوع الملف

يفضل البحث عن صيغة الملف الأكثر استخدامًا في الملفات الرسمية، وهي "filetype:pdf".

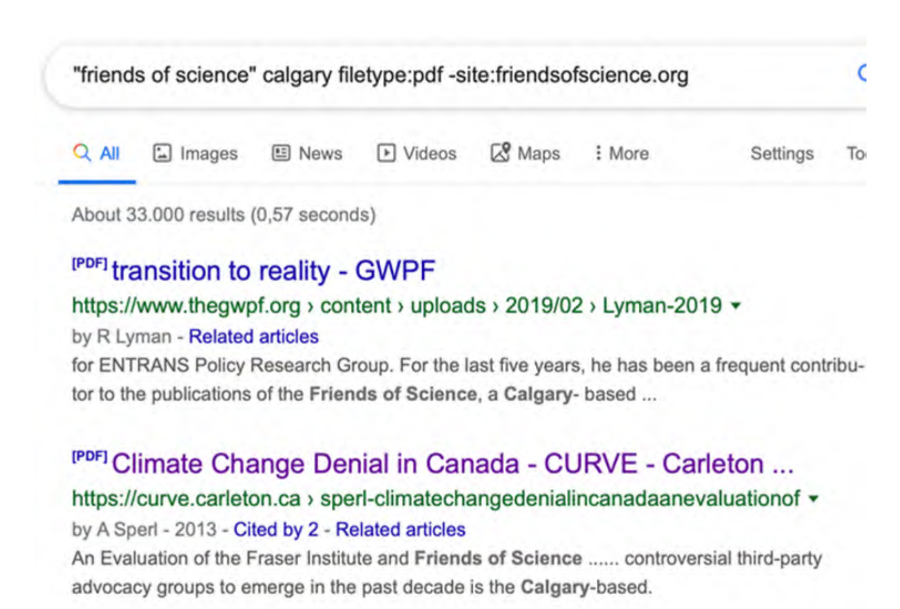
الخطوة 3: قم باستثناء الموقع الإلكتروني المستهدَف

أنت في هذه الحالة تبحث عن معلومات من أطراف خارجية، لذا سيكون من الأفضل استثناء النتائج من الموقع الإلكتروني الخاص بالجمعية، وسنقوم بذلك عبر إضافة "-site:friendsofscience.org".

و هكذا فإن صيغة البحث الكاملة ستكون كما يظهر أدناه:

"friends of science" calgary filetype:pdf -site:friendsofscience.org

وبما أننا بحثنا عن المطلوب في وثائق رسمية وليس من الموقع الرسمي للجمعية فإننا سنتمكن من معرفة بعض الجهات الداعمة للجمعية، إضافة إلى بعض الجهات التي تنتقدها:

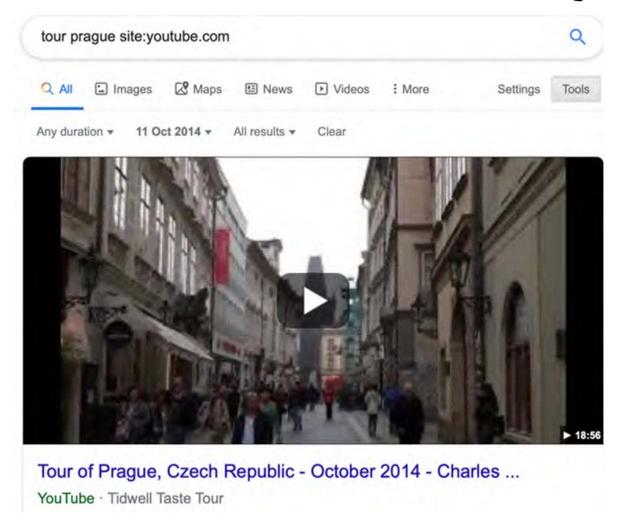


3. فلترة وسائل التواصل الاجتماعي في المصادر الأولية

يوتيوب

هنالـك خلـل فـي أداة البحـث فـي يوتيـوب، والتـي لا تسـمح بفلتـرة مقاطـع الفيديـو التـي يزيـد عمرهـا عن عـام. فـإن كنـت تريـد مثـلًا البحـث عن مقطـع فيديـو لجولـة فـي بـراغ مـن تاريـخ 11 أكتوبـر 2014، فلـن تسـتطيع عبـر البحث في المنصة تجاوز فترة العام.

ولتجـاوُزِ هـذه المشـكلة، يمكنـك إدخـال التاريـخ المطلـوب علـى محـرك البحـث جوجـل، عبـر قائمـة "أدوات" (Tools)، ثـم اختيـار "Any time"، ومـن تلـك القائمـة اختيـار تحديـد التاريـخ الدقيـق "Custom Range". وهكذا نحصل على النتائج المطلوبة:



تويتر

بالرغم من فعالية صيغة البحث "site"، إلا أنها ستخيب ظنك لو حاولت استخدامها للبحث عن معلومة في تويتر. فلنجرِّبْ مثلًا البحثَ عبر هذه الصيغة لنجد التغريدة التي ذكرتُ فيها على حسابي لأول مرة شيئًا عن "دليل التحقق":

"verification handbook" site:twitter.com/henkvaness

لكنك غالبًا لن تحصل سوى على نتيجة واحدة، وهذا ما حصل معي أثناء كتابة هذا الفصل. عادة ما تُخفِق محركات البحث العامة مثل جوجل في توفير نتائج مرضية من تريليونات التغريدات على تويتر، أو منشورات على منصات ضخمة أخرى مثل فيسبوك وإنستغرام.

لكن فيما يخص تويتر، فيمكن الاستفادة من خاصية البحث المتقدم التي تتيحها المنصة، والبحث عبر الكلمات الرئيسية، واسم المستخدم، والفترة الزمنية المطلوبة، كما في المثال الآتي:

Advanced search

Words

All of these words	verification handbook
This exact phrase	
Any of these words	
None of these words	
These hashtags	
Written in	All languages

People

From these accounts	henkvaness
To these accounts	
Mentioning these accounts	

Places

Near this place	

Dates

From this date	to 2014-12-31

Search

لا تنسَ النقر على خيار "الأحدث" (Latest) على الشريط في صفحة البحث، وذلك كي تعرض النتائج بترتيب زمني عكسي؛ لأن الوضع الافتراضي للبحث يقدِّم النتائجَ التي يعتبرها تويتر التغريدات "الأعلى".

فيسبوك

استخدام صيغة "site" على جوجل للبحث عن نتائج على فيسبوك لن يقدِّم أفضل النتائج أيضًا، لكن يمكن أيضًا الاستفادة من آلية البحث التي توفرها المنصة نفسها. فلنجربْ مثلًا البحث عن منشورات تعود لفترة مارس 2019 عن كيكة فراولة من أشخاص يقطنون في بروكلين. للقيام بذلك سنتبع الخطوات التالية:

الخطوة 1: اكتب ما تريد البحث عنه



الخطوة 2: اضغط على "منشورات" (Posts) من الشريط في صفحة البحث

Posts

الخطوة 3: حدد الموقع

TAGGED LOCATION
Anywhere
Brooklyn, New York

الخطوة 4: حدد الوقت

DATE POSTED
Any Date
2019
2018
2017
Mar 2019
Choose a Date...

وستصل إلى النتائج:



Svetlana SP

At Brooklyn, New York

Mar 20 · · Happy spring! 🌿🌹🌸🍓🌿🌺 #cake #buttercream #cakestagram #cakeart #chocolate #homemade #food #cakelover #strawberry #meringue #brooklyncakes #nyccakes #nycbaker #cakesinbrooklyn #instalike #instalove #yummy #delish #торт #красиво...





9



Baked to Enjoy party treats and sweets

Page · 221 like this · Cupcake Shop · At Brooklyn, New York

Mar 26 · · #enjoywithjay #treatyourevent #customcakes #buttercreamdreams #dripcakes #strawberrycake @ Brooklyn, New York



إنستغرام

للبحث في إنستغرام عن صور تعود لتاريخ وموقع محدّدَين، يمكنك زيارة موقعي whopostedwhat، وكتابة عملية البحث التي ترغب بالقيام بها.

Instagram - Posts on Date Tagged With Location

Displays Instagram posts at a location on a certain date or earlier. Instagram will first show you a section called "Top Posts" containing a few rows of photos generated from an algorithm. The posts by date are in the section just below, named "Most Recent", where photos are sorted chronologically, newest first. Location URL looks like: https://www.instagram.com/explore/locations/95099702/mgm-grand-las-vegas/

Posts at [Instagram location URL] on [ ] Search

Example: Find all posts from Las Vegas on July 4, 2019

الفصل الثالث: الكشف عن الحسابات الإلكترونية والذباب الإلكتروني والأنشطة السيبرانية الزائفة

جوهانا وايلد وتشارلوت غودارت

تشارلوت غودارت: صحفية استقصائية ومدربة في مؤسسة Bell-ingcat، وقد عملت قبل ذلك في مركز حقوق الإنسان في جامعة كاليفورنيا بيركلي، حيث عملت ضمن مختبر التحقيقات في المركز، إضافة إلى تدريب الطلبة على القيام بالأبحاث بالاعتماد على المصادر المفتوحة حول النزاعات في مناطق مختلفة في العالم لصالح الهيئات الإنسانية العالمية.

جوهانا وايلد: محققة مختصة بالمصادر المفتوحة في مؤسسة Bellingcat، ويتركز اهتمامها على الجوانب التقنية وتطوير الأدوات للاستخدام في التحقيقات الصحفية الرقمية، ولديها خبرة في مجال صحافة الإنترنت. عملت سابقًا مع صحفيين في مناطق صراع أو مناطق شهدت صراعات سابقة، وهي ناشطة في دعم الصحفيين في شرق أفريقيا لإنتاج مواد ونشرها مع إذاعة "صوت أمريكا".

في نهاية أغسطس 2019 قرّر بنيامين ستريك (Benjamin Strick) -وهو أحد المساهمين مع "بيلينغ كات Bellingcat" وبرنامج "عين أفريقيا" (Africa EYE) من إنتاج بي بي سي- العملَ على تحليل التغريدات التي تنشط في نشر هاشتاغ (WestPapua#) و (Free-#WestPapua)، وذلك بعد أن لاحظ عددًا من الحسابات ذات سلوك مريب. فجميع هذه الحسابات نشطت في نشر رسائل داعمة للحكومة الإندونيسية في وقت كان الصراع في بابوا الغربية قد بدأ يلفت اهتمامًا

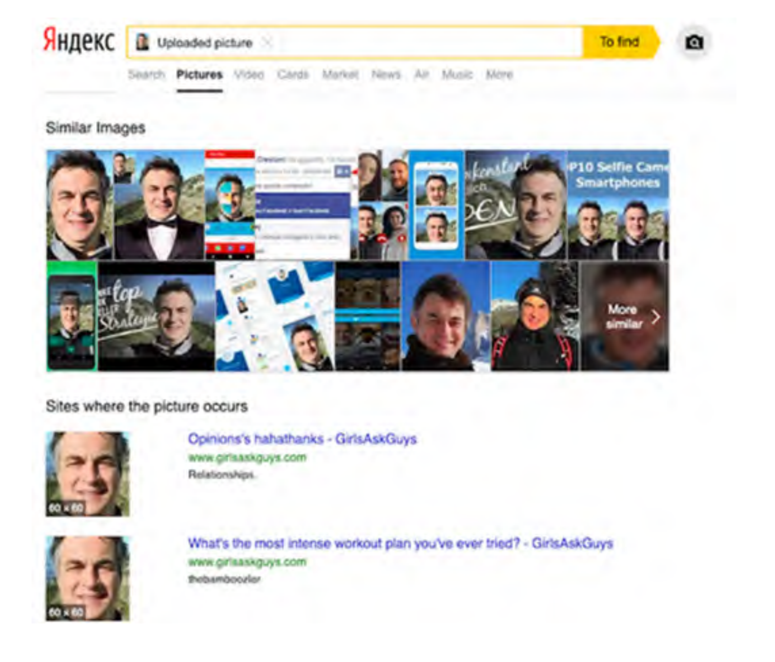
عالميًّا، وبدا أنّه ثمة حَراكٌ مطالب بالاستقلال قد خرج إلى الشوارع للمطالبة بالاستقلال عن السيطرة الإندونيسية، ما أدى إلى اندلاع مواجهات عنيفة بين الشرطة الإندونيسية والمتظاهرين.

بدا في الحسابات التي تابعها ستريك بعض الأنماط المتشابهة المثيرة للريبة، وسرعان ما بدأ يقتنع بأن ما يلاحظه ليس إلا مؤشرات أولية على سلوك جماعيّ منسّق، لكنه ظل يتابع عن كثب ويدوّن أدقّ الملاحظات.

بداية، اكتشف ستريك أن العديد من هذه الحسابات المشبوهة تستخدم صورًا مسروقة. انظر مثلًا هذا الحساب الذي يحمل اسم "ماركو":



عبر استخدام آلية البحث العكسي في محرك Yandex، تبين لستريك أن صورة البروفايل على الحساب قد استخدمت في عدة مواقع إلكترونية أخرى وتحت أسماء مختلفة، لم يكن أي منها باسم "ماركو". وهذا أثبت أن الحسابات، على أقل تقدير، ليست واضحة بشأن هوياتها.



وبالإضافة إلى فبركة الهويات، لاحظ ستريك أن الحسابات نشرت محتوى متشابهًا بل حتى متماثلًا في العديد من الحالات، إضافة إلى قيامها بإعادة التغريد فيما بينها. وما كان لافتًا بشكل خاص أيضًا هو أن بعض هذه الحسابات كانت تنشر المحتوى في وقت معيّن متكرّر بحسب ما يوضّح تحليل أنماط الرموز الزمنية للتغريدات. فعلى سبيل المثال، كان الحسابان (@bellanow1) و(@kevinma40204275) ينشران التغريدات في الدقيقة السابعة أو الدقيقة 32 من أي ساعة خلال اليوم.

26/8/19	17:07:37	bellanow1	26/8/19	23:07:20	kevinma40204275
26/8/19	5:27:06	bellanow1	26/8/19	21:32:52	kevinma40204275
26/8/19	5:27:06	bellanow1	26/8/19	20:32:52	kevinma40204275
26/8/19	5:27:05	bellanow1	26/8/19	18:32:51	kevinma40204275
26/8/19	5:27:04	bellanow1	26/8/19	15:07:22	kevinma40204275
26/8/19	5:27:04	bellanow1	26/8/19	12:32:54	kevinma40204275
26/8/19	3:32:55	bellanow1	26/8/19	9:32:54	kevinma40204275
26/8/19	0:32:56	bellanow1	26/8/19	5:32:54	kevinma40204275
26/8/19	0:07:33	bellanow1	26/8/19	5:07:36	kevinma40204275
25/8/19	23:32:54	bellanow1	26/8/19	3:32:54	kevinma40204275
25/8/19	22:32:53	bellanow1	26/8/19	0:32:54	kevinma40204275
25/8/19	22:07:06	bellanow1	25/8/19	23:32:52	kevinma40204275
25/8/19	20:32:53	bellanow1	25/8/19	23:07:16	kevinma40204275
25/8/19	10:07:19	bellanow1	25/8/19	19:32:53	kevinma40204275
25/8/19	9:32:56	bellanow1	25/8/19	15:07:24	kevinma40204275
25/8/19	9:07:27	bellanow1	25/8/19	10:32:55	kevinma40204275
25/8/19	8:32:56	bellanow1	25/8/19	7:32:55	kevinma40204275
25/8/19	7:07:23	bellanow1	25/8/19	6:32:54	kevinma40204275
25/8/19	6:32:56	bellanow1	25/8/19	6:08:01	kevinma40204275
24/8/19	13:07:57	bellanow1	25/8/19	3:07:21	kevinma40204275
24/8/19	10:07:19	bellanow1	25/8/19	0:07:26	kevinma40204275
24/8/19	7:32:56	bellanow1	24/8/19	20:32:51	kevinma40204275
24/8/19	7:07:20	bellanow1	24/8/19	20:07:08	kevinma40204275
24/8/19	5:32:56	bellanow1	24/8/19	19:32:51	kevinma40204275
24/8/19	4:32:56	bellanow1	24/8/19	15:07:24	kevinma40204275
24/8/19	0:07:31	bellanow1	24/8/19	13:32:55	kevinma40204275
			24/8/19	10:07:17	kevinma40204275
			24/8/19	7:32:54	kevinma40204275
			24/8/19	7:07:18	kevinma40204275
			24/8/19	5:32:54	kevinma40204275
			24/8/19	1:32:54	kevinma40204275

ومن المستبعد أن يلتزم إنسان بهذا النمط المتسق من التغريد. فهذه المزامنة عبر حسابات متعددة، بالإضافة إلى الصور المضللة التي تستخدمها، أدلة قد تشير إلى أن هذه الحسابات وهمية غير مرتبطة بهويات أشخاص حقيقيين، وأنها قد تكون آلية. وعبر مواصلة تحليل مثل هذه الأنماط

المشبوهة من السلوكيات الرقمية، توصل ستريك إلى أن هذه الحسابات كانت جزءًا من شبكة حسابات آلية ذات بروباغندا داعمة للحكومة الإندونيسية، وكانت تنشر معلومات متحيّزة ومضللة بخصوص الصراع في بابوا الغربية (يمكن قراءة المزيد حول هذه الشبكة الأكبر المنظمة لهذه الحسابات في دراسة الحالة الثانية في الفصل الحادي عشر).

ما هو الحساب الآلي؟ الجواب عن هذا السؤال أكثر تعقيدًا مما تتوقع

الحالة في بابوا الغربية ليست بطبيعة الحال أول ولا آخر عملية تضليل معلوماتي تعتمد على الحسابات الآلية على وسائل التواصل الاجتماعي. فثمة العديد من العمليات الأخرى التي افتُضح أمرها على نطاق أوسع بكثير ونالها قدْر كبير من الانتقادات والمتابعة، لكن في جوهر النشاط الملاحظ فإنها تتشارك مع حالة بابوا الغربية في طريقة العمل.

الحساب الآلي هو تطبيق برمجي يقوم آليًّا بمهامّ تحدِّد طبيعتها أطرافٌ بشرية، وعليه فإن الحساب الآلي قد يقوم بمهمة حميدة أو خبيثة اعتمادًا على مقاصد هذه الأطراف التي "تملكه".

الحسابات الآلية التي عادة ما تكون موضوع النقاشات العامة هي حسابات آلية تنشط على وسائل التواصل الاجتماعي، مثل فيسبوك وتويتر ولينكد إن، حيث يمكن توظيفها من أجل نشر رسائل أيديولوجية معينة، وعادة ما يكون ذلك بهدف إثبات أن ثمة قاعدة واسعة من الدعم والتأييد، لموضوع ما أو شخص أو محتوى معين أو وسم (هاشتاغ).

ويمكن تصنيف الحسابات الآلية على وسائل التواصل الاجتماعي في ثلاث فئات رئيسية:

حسابات آلية للجدولة (The Scheduled bot) وحسابات آلية للمراقبة

(The Watcher bot) وحسابات آلية للترويج (The Amplifier bot)

ومن الضروري تحديد نوع الحسابات الآلية التي ترغب بتعقبها ودراستها، وذلك لأن لكلّ من هذه الأنواع غرضًا خاصًا، ولكل غرض نمطًا مختلفا من اللغة وشكل التواصل. لكن إنْ كنّا مهتمين بالحديث عن المعلومات المضللة، فإنّ ما يلزمنا البحث فيه هو الحسابات الآلية الخاصة بالترويج.

حسابات الترويج الآلية غرضُها واضح من اسمها: الترويج لمحتوى ما وتضخيم انتشاره، بهدف التأثير على الرأي العام في وسائل التواصل الاجتماعي. كما يمكن استخدامها من أجل تشكيل صورة عن بعض الأفراد أو المؤسسات تُوهِم بأنها تتمتع بقاعدة شعبية واسعة من المتابعين بخلاف ما عليه الواقع، فقوّة هذه الحسابات تعتمد على لغة الأرقام.

قد تعمل شبكة من حسابات الترويج الآلية على تصعيد وسوم (هاشتاغ) معينة، ونشر روابط أو محتوى بصري ما، أو استهداف شخصية ما والتهجم عليها عبر الإنترنت في محاولة لتشويه سمعتها أو لإثارة الشكوك والجدل حولها.

ومن خلال العمل الموحّد بأعداد كبيرة، تعطي هذه الحسابات الآلية انطباعًا بأنها حقيقية، ما يجعلها قادرة على اكتساب دور في تشكيل الرأي العام. وتعتمد هذه الحسابات بشكل أساسيّ في عمليات بث المعلومات المضللة على حملات تصعيد الوسم، أو عبر المشاركة المكثفة للأخبار على شكل روابط أو مقاطع فيديو أو ميمات أو صور أو غير ذلك من أشكال المحتوى. ففي حملات تصعيد وسم ما، تقوم الحسابات الآلية بنشر تغريدات تتضمن وسمًا معينًا واحدًا أو مجموعة من الوسوم، في حملة منسقة بينها. أما الهدف من هذه العملية فهو التأثير على الخوارزمية الخاصة بتصعيد الوسوم في تويتر، بحيث يظهر وسم ما على قائمة الوسوم المتصدّرة. مثال ذلك هو وسم (#Hillarysick)، والذي انتشر على نطاق واسع بفعل الحسابات الآلية، وذلك بعد أن

تعثرت هيلاري كلينتون وكادت تسقط في سبتمبر 2016، وذلك قبيل موعد الانتخابات الرئاسية في الولايات المتحدة.

ومن الضروري الإشارة هنا إلى أن حملات تصدير الوسوم لا تتطلب الاستعانة بحسابات آلية بالضرورة، بل قد تكون أكثر فعالية بدونها. يمكن الاطلاع على هذا التحقيق لقراءة المزيد عن "مولّدي الوسوم" غير الآليين.

من السهل عمومًا شراء وإنشاء الحسابات الآلية، فثمة العديد من المواقع التي يمكن أن تزودك بجيش من الحسابات الآلية مقابل بضع مئات من الدولارات أو أقل. لكن الصعوبة تكمن في امتلاك وإدارة حسابات آلية ذات نمط أكثر تعقيدًا من السلوك وأقدر على الحفاظ على "سمة" بشريّة لضمان تأثير أكثر فعالية.

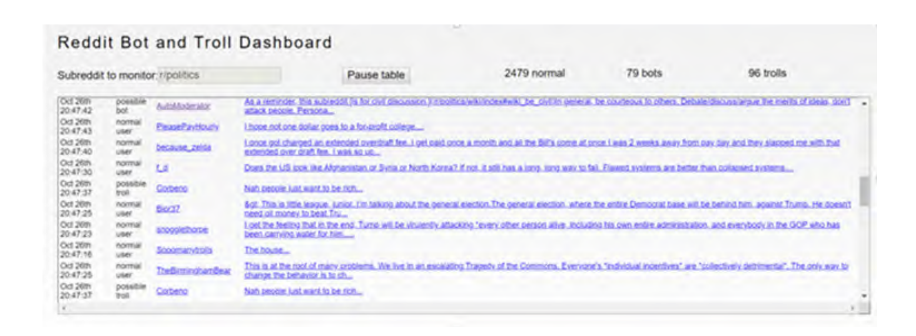
كيف تكشف عن الحسابات الآلية؟

أنشأ المطورون والباحثون مؤخرًا العديد من الأدوات للمساعدة في معرفة ما إذا كان أحد الحسابات وهميًا. هذه الأدوات رغم فائدتها في جمع المعلومات، إلا أن النتيجة التي تُوفِّرها ليست قطعية، ولا يمكن الاعتماد عليها كأساس ينطلق منه الصحفي في إعداد تقاريره أو للتوصل إلى أي خلاصة.

أحد أبرز هذه الأدوات هو موقع Botometer، من تطوير مجموعة من الباحثين في جامعة إنديانا. تقدم هذه الأداة -وفق عدد من المعايير المختلفة- تقييمًا لأي حساب على تويتر ومدى احتمال أن يكون ومن فيه من المتابعين حسابًا آليا.



قـام جيسـون سكورونسـكي بإنشـاء لوحـة تفاعليـة خاصـة لحسـابات موقـع "Reddit"، بحيـث تقيّـم هـذه اللوحـة مـاذا إذا كانـت التعليقـات علـى أي حسـاب فـي الموقـع هـي تعليقـات صـادرة عـن حسـابات آليـة أم مـن أشـخاص عاديين.



لكـن معظـم الأدوات المتوفـرة للكشـف عـن الحسـابات الآليـة عبـر الإنترنـت هـي أدوات موجّهـة لمنصـة تويتـر بشـكل خـاص، باسـتثناء أمثلـة قليلـة. والسـبب هـو أن العديـد مـن منصـات التواصـل الاجتماعـي، بمـا فـي ذلـك فيسـبوك، تفـرض قيـودًا علـى واجهـة برمجـة التطبيقـات (API)، بطريقـة تمنـع العامـة مـن تحليـل البيانـات واسـتخدامها بطريقـة تسـمح بإنشـاء مثـل هذه الأدوات الخاصة بالتحقق.

أؤكّـد مجـددًا علـى أن أدوات الكشـف عـن الحسـابات الآليـة قـد تكـون نقطـة استـئناس مبدئيـة وحسـب، ولا يمكـن الاعتمـاد عليهـا كليًّـا للتوصـّل إلـى نتائـج قطعية.

أمـا السـبب وراء التبايـن فـي دقّـة النتائـج التـي تقدمهـا هـذه الأدوات فيعـود إلـى حقيقـة بسـيطة، وهـي أنـه لا تتوفّـر قائمـة نهائيـة بالمعاييـر الخاصـّة بالكشـف عـن الحسـاب الآلـي بدقّـة يقينيـة. كمـا أن ثمـة خلافـات واسـعة بشـأن كيفية الحكم على حساب ما بأنه آلي.

بعـض الباحثيـن فـي مشـروع "البروباغنـدا الآليـة" التابـع لمعهـد أكسـفورد

للإنترنت يصنف الحسابات التي تنشر أكثر من 50 منشورًا في اليوم على أنها مرتبطة بعملية "أتمتة عميقة". أما مختبر الأبحاث الجنائية الرقمية في المجلس الأطلنطي فيرفع هذا الرقم إلى 72 تغريدة في اليوم لاعتبار الحساب مشبوهًا بنسبة معقولة (تغريدة واحدة كل 10 دقائق على فترة 12 ساعة متواصلة)، أما في حال تجاوز العدد 144 تغريدة في اليوم فيكون مشبوهًا بنسبة أعلى.

وعادة ما يكون من الصعب تحديد ما إذا كان يقف وراء حملة معلومات مضللة حسابات آلية أو حسابات يديرها أشخاص حقيقيون لديهم حافز ما أو يحصلون على مقابل مالي لقاء نشر محتوى مكثف حول موضوع ما.

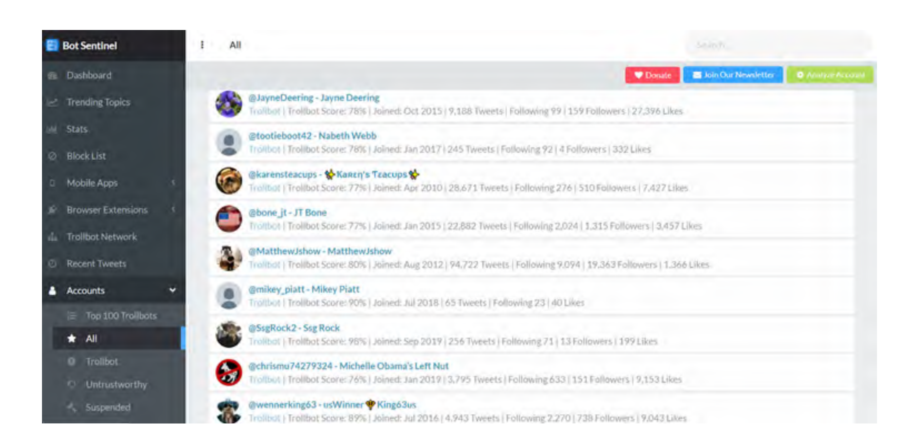
لقد اكتشفت بي بي سي في أحد التحقيقات أن الحسابات التي كانت تنشر رسائل متماثلة على فيسبوك ذات محتوى داعم لبوريس جونسون في نوفمبر 2019 كانت حسابات يديرها أشخاص حقيقيون حاولوا أداء دور الحسابات الآلية على وسائل التواصل الاجتماعي.

هنالك أيضًا حسابات السايبورغ (Cyborg)، أو "الكائنات السيبرانية"، وهي حسابات على وسائل التواصل الاجتماعي مؤتمتة جزئيًا فقط، ويمكن للبشر التحكم بها، ويلاحَظ في سلوكها سماتٌ بشرية طبيعية وأخرى آلية.

ومن الضروري أن يتجنب الصحفيون وصف حسابات مشبوهة بأنها "حسابات آلية" دون امتلاك الدليل الكافي والمقنع، وذلك لأن أي اتهام غير دقيق من شأنه تقويض مصداقية الجهد الصحفي المبذول.

إحدى الطرائق الممكنة للتعامل مع هذه الأنواع المختلفة من الحسابات الآلية، وحسابات السايبروغ، والحسابات البشرية ذات النشاط الرقمي المفرط، تكون بالتركيز أثناء عملية التحقيق على مراقبة جميع أشكال السلوك الذي يظهر سمات آلية أو وهميّة، بدل التركيز حصرًا على اكتشاف نوع بعينه من الحسابات المشبوهة.

لدينـا مثـلًا أداة "[Bot Sentinel]"، والتـي توفـر قاعـدة بيانـات متاحـة للاسـتخدام العـام تشـتمل علـى حسـابات تويتـر (فـي الولايـات المتحـدة) ذات السـلوك المريـب. وقـد كان هـدف الأشـخاص الذيـن طـوروا هـذه الأداة هـو جمـع "الحسـابات التـي تكـرّر خرقهـا للقواعـد المعمـول بهـا فـي تويتـر"، ولـم يبحثوا بشكل مقصود عن حسابات يشكّون بأنها آلية.



خطـوات التحقـق مـن السـلوك المشـبوه علـى وسـائل التواصل الاجتماعي

نقتـرح -كآليـة عامـة- اتبـاعَ هذه الخطـوات عند محاولـة التحقق من السـلوك الموجّه أو الآلي على شبكات التواصل الاجتماعي:

1. المتابعة الدقيقة للحسابات ذات السلوك المشبوه.

2. الاسـتئناس بنتيجـة الفحـص عبـر الأدوات الخاصـة بالكشـف عن الحسـابات الآلية أو عمليات التحليل التقنية الأكثر تعقيدًا.

3. التحـرّي عـن أنشـطة هـذه الحسـابات، ومحتواهـا، وشـبكة الحسـابات التـي تتفاعـل معهـا، إلـى جانـب أسـاليب التحقيـق الصحفـي التقليديـة؛ مثـل محاولـة التواصـل مـع هـذه الحسـابات، أو مـع الأشـخاص الذيـن يدّعـون أنهـم يعرفـون أصحابها.

4. استشارة خبراء متخصصين في الحسابات الآلية والنشاط الوهمي على وسائل التواصل الاجتماعي.

من أجل معرفة كيفية التحقق "اليدوي" من الحسابات المشبوهة، فإنه من الضروري الإحاطة بالمؤشرات الأولية التي تدل على أنك قد تكون تتعامل مع حسابات آلية على تويتر أو سواها من وسائل التواصل الاجتماعي.

فلنتذكّر أن كل حساب آلي على وسائل التواصل الاجتماعي يحتاج مبدئيًا إلى "هوية"، إذ يحرص الطرف الذي ينشئ هذه الحسابات على اختيار هويّة مقنعة إلى حد كبير، لكن إنشاء حساب آلي بمثل هذه الهويّة وتطويرها بشكل مستمر ليس بالأمر السهل ويتطلب بعض الوقت، خاصة في حال كان الهدف إنشاء شبكة ضخمة من الحسابات الآلية. فكلما زاد عدد الحسابات التي تديرها جهة ما، زاد العبء المترتب عليها في إدارتها وتطوير هويتها بالشكل الذي يضمن أن تكون مقنعة، ويبعد عنها شبهة الشكّ في كونها حسابات آلية. وهذه هي نقطة الضعف في الحسابات الآلية، وهي الجانب الذي عادة ما تنكشف من خلاله. في العديد من الحالات نجد أن من ينشئ الحسابات الآلية لا يضع الوقت الكافي لبناء الحساب وتشكيل هويته المقنعة، وهذا ما يسعى المحققَ الجيدَ الكشفُ عنه.

وإليك بعض العناصر التي يجدر التنبه إليها:

عدم استخدام صورة شخصية للبروفايل

كثيرًا ما يكون استخدام صورة بروفايل مسروقة (كما لاحظنا في مثال بنيامين ستريك في التحقيق الخاص ببابوا الغربية) أو عدم استخدام أي صورة، مؤشرًا أوليًّا على أن الحساب مشبوه على الأقل. وبما أنّ مَن ينشئون الحسابات الآلية يرغبون في إنشاء العديد من الحسابات في وقت واحد، فإنه يلزم أن يكون في حوزتهم مجموعة من الصور، وعادة ما يفعلون ذلك عبر سرقتها من مواقع أخرى. هنا قد تحدث بعض أنواع

التضـارب. فمثـلًا، قـد تجـد علـى حسـاب مـا صـورة لرجـل، ولكـن اسـم المسـتخدم هـو اسـم أنثـى، وهـذا كفيـل بإثـارة الشـكّ بالحسـاب. وفـي العديـد مـن الحـالات الأخـرى، يسـتخدم مـزوِّرو الحسـابات الآليـة رسـمات عامـة أو صـورًا لحيوانـات، وهـذا كذلـك أسـلوب صـار نمطًـا معروفًـا فـي الحسـابات الآليـة، ويمكـن وضعـه بالحسـبان دائمًـا أثنـاء البحـث عـن حسـابات آليـة أو مشبوهة.

التوليد الآلي لأسماء المستخدم

بعـد التدقيـق فـي الصـور ننتقـل إلـى النظـر فـي الأسـماء واسـم المسـتخدم (Username). مـن المعـروف أن كل حسـاب علـى تويتـر لـه اسـم مسـتخدم فريـد بـه، مـا يعنـي أن العديـد مـن الأسـماء التـي ترغـب باسـتخدامها سـتكون محجـوزة بالفعـل ويلزمـك البحـث عـن اسـم مسـتخدم خـاص غيـر مسـتخدم مـن قبـل، وهـو مـا يشـكّل تحديًـا حقيقيًـا علـى جهـة ترغـب فـي إنشـاء 50 أو 500 أو 5000 حسـاب آلـي خـلال فتـرة قصيـرة مـن الوقـت. وعـادة مـا يتّبـع منشـئو الحسـابات الآليـة إسـتراتيجية تسـاعدهم علـى العثـور -بيسـر وسـرعة- علـى أسـماء مسـتخدم شـاغرة، وذلـك عبـر كتابـة معـادلات لتوليـد أسـماء مستخدم بشكل آلي:

Username followed by a 4 digit number	12 random characters in length which can consist of (a-zA-Z and 0-9)	Any first name followed by a random eight-digit number, indicating that the default username generated by Twitter has been used.
superman_1230 superman_2313 superman_9832 superman_3934 superman_4920	vP1tfl1ZoPG1 dNi29j2utANQ YQBrodhbPC84 TUq3R6GBWYyA XI87NreGshx8	Neil03121977 Sarah92839820 Claire02938593 John09340293 Stephen83749284

عنـد ملاحظـة عـدة حسـابات علـى تويتـر أسـماء المسـتخدم الخاصـة بهـا تتألف مـن نفـس عـدد الخانـات مـن الحـروف والأرقـام، يمكنـك البحـث يدويـا عـن المزيـد مـن هـذه الحسـابات التـي تتبـع هـذا النمـط فـي أسـماء المسـتخدم

(الهاندل) في قائمة المتابعين، وربما تتمكن من تحديد شبكة من هذه الحسابات.



في هذا المثال، نلاحظ أن الحسابات تشترك بعنصر آخر فيما بينها، وهو أنها جميعًا أنشئت في سبتمبر 2019. فإذا تتبعنا المؤشرات الأخرى وتحققنا منها، فإن ذلك قد يكون دليلًا إضافيًا على أن الحسابات قد أنشئت في وقت واحد ومن قِبل جهة واحدة.

حجم نشاط الحساب غير متناسب مع عمره

عليك أن تكون أكثر حذرًا وريبة في حال ملاحظة وجود حساب أنشئ حديثًا لكن عدد متابعيه أو عدد التغريدات التي نشرها كبير نسبيًا بالنسبة لعمره. كما عليك التنبه أيضًا في حال ملاحظة حساب قديم بعدد قليل من المتابعين بالرغم من النشاط الكبير في التغريد.

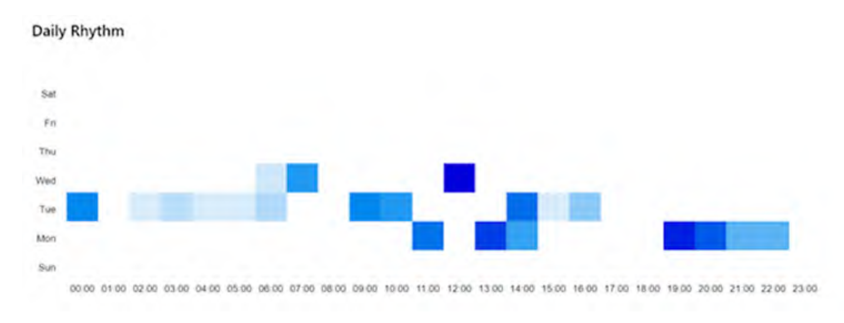


وفـي حـال وقعـت علـى حسـاب تنطبق عليـه هذه الملاحظات، قم بدراسـة نشـاطه فـي التغريـد بشـكل معمـق. بحِسـبة بسـيطة، اقسـم عـدد التغريـدات حسـبما يظهر فـي صفحـة حسـابه علـى عمـر الحسـاب النشـط بالأيـام. فمثـلًا، لـو كان لدينـا حسـاب نشـر 3,489 تغريدة حتى 11 نوفمبر 2019، وكان الحسـاب قد أنشـئ فـي 15 أغسـطس 2019، فسـنقوم بقسـمة الرقـم 3,849 علـى 89 يومًـا (عـدد الأيام التي كان فيها الحساب نشطًا)، والنتيجة هي 39.2 تغريدة في اليوم.

وبعـد ذلـك نقـوم بفحـص تقديـري للتغريـدات التـي نشـرها الحسـاب منـذ إنشـائه، لمحاولـة التأكد إن كان هـذا العـدد مـن التغريـدات كبيـر جـدًا أو غيـر واقعي أو لا يمكن لحساب بشري القيام به بشكل مستدام.

أنماط مشبوهة من التغريد

أحـد العناصـر الأخـرى التـي تلزمنـا دراسـتها هـو نمـط التغريـد المتبـع فـي الحسـاب. قـد يكـون للبشـر تفضيـلات عامـة فيمـا يتعلـق بالأيـام أو الأوقـات التـي ينشـرون فيهـا تغريداتهـم، لكـن مـن المسـتبعد أن تجـد شـخصًا يغـرّد بشـكل حصـري يـوم الإثنيـن والثلاثـاء والأربعـاء، ولا يغـرّد أبـدًا فـي الأيـام الأخـرى. ويكـون هـذا النمـط حاصـلًا علـى فتـرة ممتـدة مـن عمـر الحسـاب. وللحصـول علـى عـرض بصـريّ لأنمـاط تغريـد حسـاب مـا، يمكـن اسـتخدام هذه الأداة الخاصة بتحليل نشاط الحساب من تطوير لوكا هامر:

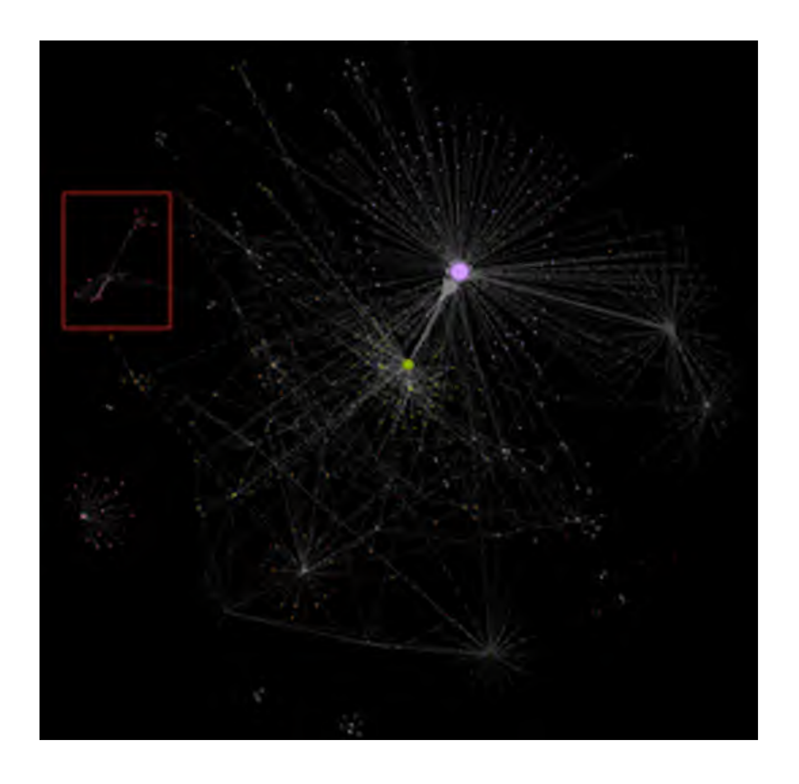




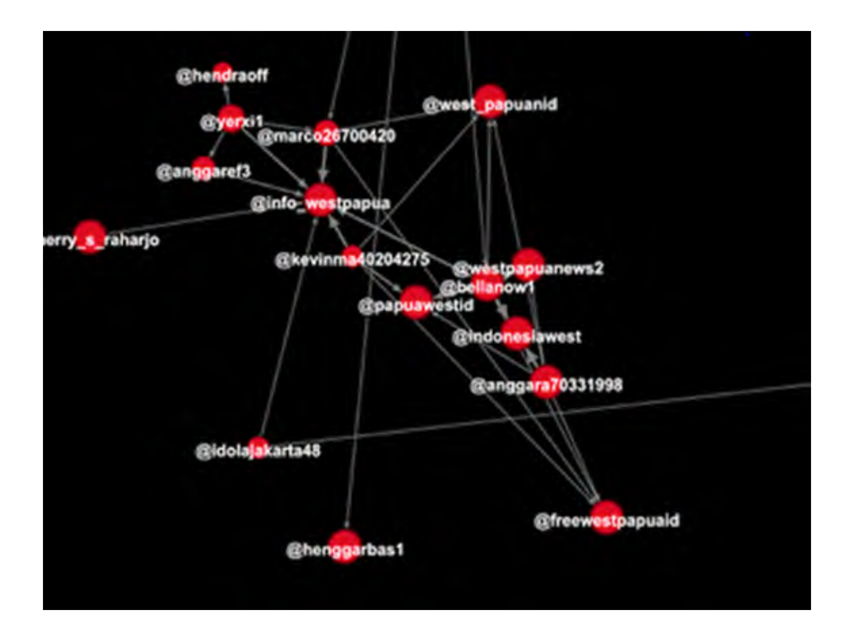
العرض التصويري للبيانات في عملية التحقيق

يمكن من أجل الحصول على فهم أفضل لنشاط شبكة من الحسابات الآلية استخدام منصة للعرض البصري للبيانات مثل Gephi. لقد استخدم بنيامين ستريك المساهم في مؤسسة Bellingcat هذه الأداة في تحليل أشكال الارتباط بين عدة حسابات على تويتر يشتبه في كونها شبكة من حسابات آلية مؤيدة لأندونيسيا.

وبالاستفادة من هذا العرض البصري للروابط بين مجموعة كبيرة من الحسابات على تويتر، لاحَظ ستريك أن ثمّة نمطًا لافتًا في الجانب الأيسر من الصورة (باللون الأحمر).



وعبر تكبير ذلك الجانب من الصورة، تمكن من تحديد حسابات تويتر التي كانت جزءًا من تلك الشبكة.



كل دائـرة مـن هـذه الدوائـر الحمـراء تشـير لحسـاب علـى تويتـر، أمـا الخطـوط فتشـير إلـى الارتباطـات فيمـا بينهـا. عـادة مـا تظهـر الحسـابات الأصغـر فـي دائـرة أكبـر فـي منتصـف الشـكل البيانـي، مـا يعنـي أنهـا جميعًـا تتفاعـل مـع الحسـاب المؤثـر. لكـن الحسـابات فـي الشـكل أعـلاه لـم تتفاعـل بهـذه الطريقـة فيمـا بينهـا، وقـد عـزّز ذلـك مـن قناعـة سـتريك بأهميـة مواصلـة تحليـل السلوك المريب لهذه الحسابات.

مستقبل الحسـابات الآليـة علـى وسـائل التواصـل الاجتماعـي: هـل يمكن التفوق عليها؟

باتـت الحسـابات الآليـة تعتمـد علـى تقنيـات أكثـر تعقيـدًا وتطـورًا في السـنوات الأخيـرة، حيـث صـارت هـذه البرمجيـات الصغيـرة قـادرة بشـكل أكبـر علـى محـاكاة السـلوك الرقمـي البشـري. وقـد وصلنـا إلـى مرحلـة مـن هـذا التطـور تجعـل البعـض يتوقـع أن الحسـابات الاصطناعيـة سـتكون قـادرة علـى الانخـراط فـي عمليـات تواصـل رقميـة معقـدة دون أن يكتشـف طـرف المحادثة البشري أنه في الواقع يتحدث مع حسابات آلية!

لكن في الوقت الراهن ليس ثمّة دليل على وجود حسابات آلية على وسائل التواصل الاجتماعي بهذا القدر من التعقيد المرتبط بتقنيات تعلم الآلة والذكاء الاصطناعي، ويظهر لنا أن معظم حملات التضليل المعلوماتي تعتمد على حسابات ترويج آلية بتقنيات أقل تعقيدًا.

يقول الدكتور أولا بوتز (Ole Putz)، الباحث في مشروع "حسابات آلية غير متحيّزة لبناء جسور التواصل" في جامعة بيلفيلد الألمانية، إنه لا يرجح وجود حسابات آلية معقدة على وسائل التواصل الاجتماعي قادرة على إجراء حوارات حقيقية مع الناس وإقناعهم بتبني مواقف سياسية معينة. ويرى بوتز أن الطريقة الأفضل للمساعدة على كشف السلوك الموجّه على شبكات التواصل الاجتماعي تتمثل في استخدام طرائق تأخذ بالاعتبار والتحرّي كافة العوامل التي تثير الشكّ في حساب ما، كأن نلاحظ مثلًا حسابًا ما يستخدم آلية محددة لإعادة تغريد بعض الأخبار، ويقوم بمتابعة آخرين بشكل آلي، ولا يستخدم في تغريداته العناصر اللغوية التي يستخدمها البشر عادة.

وهكذا فإن التحليل المنهجي لسلوك الحساب وما فيه من محتوى وأشكال تفاعل وأنماط سلوك، هو السبيل الأفضل حتى الآن للكشف عن شبكات الحسابات الآلية.

في الفصل الخاص بدراسة الحالة سنقدم المزيد من التوضيحات والتفاصيل التقنية حول الطرائق التي اتبعناها في تحليل الجوانب المختلفة في شبكة حسابات مشبوهة على تويتر ذات علاقة بالاحتجاجات في هونغ كونغ.

دراسة حالة: الوصول إلى أدلة على وجود نشاط لحسابات آلية على تويتر خلال احتجاجات هونغ كونغ

تشارلوت غودارت، جوهانا وايلد

تشارلوت غودارت: صحفية استقصائية ومدربة في مؤسسة Bellingcat، وقد عملت قبل ذلك في مركز حقوق الإنسان في جامعة كاليفورنيا بيركلي، حيث عملت ضمن مختبر التحقيقات في المركز، إضافة إلى تدريب الطلبة على القيام بالأبحاث بالاعتماد على المصادر المفتوحة حول النزاعات في مناطق مختلفة في العالم لصالح الهيئات الإنسانية العالمية.

جوهانا وايلد: محققة مختصة بالمصادر المفتوحة في مؤسسة Bellingcat، ويتركز اهتمامها على الجوانب التقنية وتطوير الأدوات للاستخدام في التحقيقات الصحفية الرقمية، ولديها خبرة في مجال صحافة الإنترنت. عملت سابقًا مع صحفيين في مناطق صراع أو مناطق شهدت صراعات سابقة، وهي ناشطة في دعم الصحفيين في شرق أفريقيا لإنتاج مواد ونشرها مع إذاعة "صوت أمريكا".

في أغسطس 2019، أعلنت تويتر حذفها آلاف الحسابات التي قالت بأنها أسهمت في الترويج لمعلومات مضللة بخصوص احتجاجات هونغ كونغ، وأن هذه الحسابات كانت جزءًا من "عملية منسقة مدعومة من إحدى الدول". أعقب ذلك إقدام فيسبوك ويوتيوب على إصدار بيانات مماثلة تؤكّد أنها حذفت عددًا من الحسابات التي كانت منخرطة في عمليات موجّهة ومنسّقة ذات علاقة بالاحتجاجات.

لكن الفرق في الخطوة التي أقدمت عليها تويتر، هو أنها نشرت أيضًا قائمة بالحسابات التي حذفتها، ما منح المراقبين والمهتمين فرصة للتحقق بشكل أكبر في نشاطها المشبوه، وهو أمر لم تقم به فيسبوك ولا يوتيوب. وبالتعاون مع أحد المشاركين في إحدى ورش العمل التي نظمتها "Bell-ingcat"، قرر فريقنا البدء بعملية تحقق من بقية المحتوى الخاص بالاحتجاجات في هونغ كونغ؛ سعيًا وراء الكشف عن أي مؤشرات تدلّ على وجود سلوك موجّه غير طبيعي على المنصة.

تحديد النشاط المشبوه

انطلقنا من نقطة البداية، وهي البحث عن الوسوم الخاصة بالاحتجاجات. وعبر عملية بحث بسيطة باستخدام عبارة "Hong Kong Riots" (الشغب في هونغ كونغ) ظهرت لنا أعداد كبيرة من التغريدات، بعضها يشتمل على عدة وسوم.

كان هدفنا التركيز على الحسابات الداعمة للرواية الصينية، وهي تلك الشبيهة بالحسابات التي حذفتْها تويتر بناء على نشاطها الآلي، وحاولنا البحث بعبارات من قبيل "Shame on Hong Kong Police/Gov-ernment". فتوصلنا في نتائج البحث إلى عبارات مشابهة، ولكن من دون أن تشتمل على "الشرطة" أو "الحكومة". كان هدفنا هو استثناء النتائج التي تندد بموقف الحكومة أو القوات الأمنية، من أجل البحث في التغريدات التي كانت تنتقد المتظاهرين وتشوّه موقفهم. بحثنا أيضًا عن عبارات مثل "Hong Kong roaches" (صراصير هونغ كونغ)، و"Hong Kong mobs" (زعران هونغ كونغ)، وهي أوصاف كانت تنتشر في تغريدات من حسابات مؤيدة للصين.

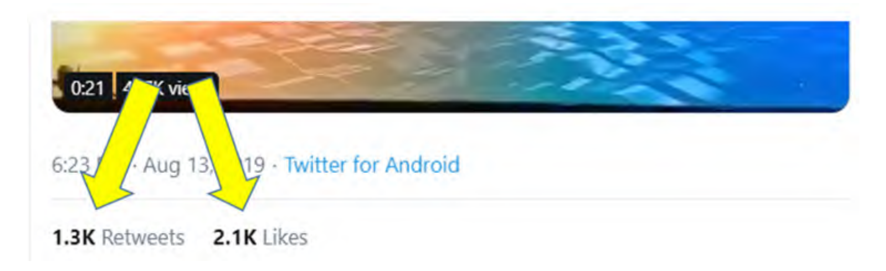
وباستخدام هذه العبارات وغيرها في عملية البحث، اطلعنا على العديد من التغريدات الأحدث حول هونغ كونغ والتي حازت على تفاعل كبير بالإعجابات وإعادات التغريد. يمكن تصفية النتائج حسب التفاعل معها،

بإضافة "min_retweets:500" أو "min_faves:500" للحصول على التغريدات التي حازت على 500 إعجاب أو إعادة تغريد على الأقل.

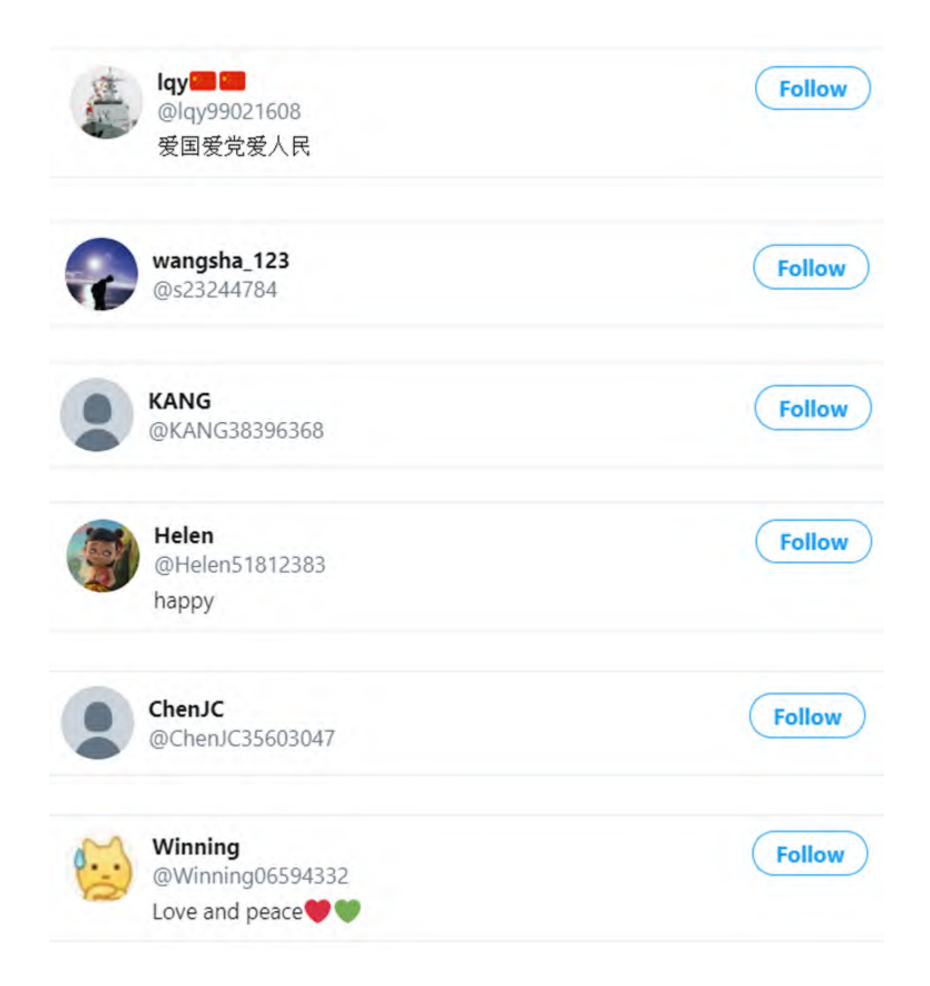
نظرنا بعد ذلك إلى الحسابات التي تفاعلت مع هذه التغريدات. وجدنا مثلًا هذه التغريدة في حساب موثّق باسم "هو تشيجن"، والذي يشغل منصب رئيس تحرير النسختين الصينية والإنجليزية من صحيفة "ذا غلوبال تايمز"، وهي إحدى الوسائل الإعلامية الممولة من الحكومة الصينية:



استعرضنا "إعادات التغريد" و"الإعجابات" على التغريدة، للاطلاع على قائمة الحسابات التي شاركت في الترويج للتغريدة.



كانت فرضيتنا هي أن الحسابات الآلية الموالية للصين ستؤدي مهمة الترويج لشخصيات إعلامية محسوبة على الحكومة الصينية. لكن في هذه الحالة، العديد من أسماء المستخدم كانت لافتة، وذلك لأنها جميعها كان تحمل أرقامًا من ثماني خانات بعد الاسم، ما يدل على أن المستخدم وافق على اسم المستخدم الافتراضي الذي يظهر تلقائيًا عند التسجيل كمستخدم جديد في المنصة، وقد استلزمَت هذه الملاحظةُ أنْ نجري المزيد من التحري عن سلوك هذه الحسابات وسماتها.

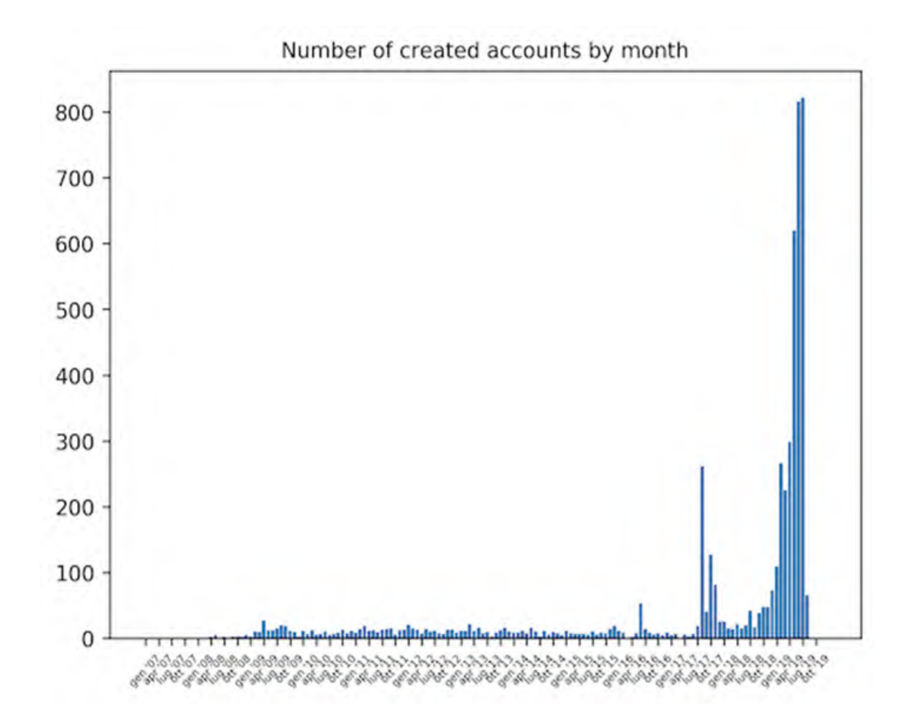


حين نظرنا في هذه الحسابات وجدنا أن عدد المتابِعين والمتابَعين قليل جدًا، ولم يُدرج أيُّ وصف تعريفي لها، وليس لها تقريبًا أي تغريدات،

ونشـاطـها الأساسـي يتمثـل فـي إعـادة التغريـد مـن حسـابات أخـرى، لمحتـوى لا علاقة له سوى بمناهضة الاحتجاجات.

لاحظنـا كذلـك أن تواريـخ إنشـاء هـذه الحسـابات كان حديثًـا، ومعظمهـا فـي أغسـطس 2019. وبمـا أن تويتـر قـد كشـفت عـن قائمـة بالحسـابات الآليـة المواليـة للصيـن بعـد أن حذفتهـا، فقد تمكنـا مـن النظـر فـي تواريـخ إنشـائها، والتأكد إن كان ثمة ارتباط فيما بينها في هذا الجانب.

وبمسـاعدةٍ مـن لويغـي غوبيلـو، وهـو مبرمـج لـه نشـاطات واسـعة فـي مجتمـع المصــادر المفتوحــة علــى الإنترنــت، اســتخدمْنا نــص بايثــون "Python script" (ويمكـن العثـور علـى الكـود علـى حسـابه علـى GitHub كمـا يمكـن معرفـة المزيـد عنـه علـى هـذا الرابـط) لتحديـد أيـة أنمـاط فـي البيانـات. يُظهـر الشـكل أدنـاه أن الحسـابات المحذوفـةَ كانـت جميعُهـا قـد أنشـئت مـن فتـرة قريبـة لا تزيـد علـى بضعـة أشـهر، وهـي تشـترك فـي ذلك مع الحسـابات النشطة الأخرى التي نتحقق من أمرها.



أتمتة العملية

بعد تحديد عينة من التغريدات والحسابات التي تثير الريبة في سماتها وسلوكها، أردنا القيام بعملية تحليل أكبر، وقد لزمَنا الاعتماد على بعض الأتمتة. حصلنا على مساعدة من أحد المشاركين في ورشة عمل في Bellingcat له معرفة بتطوير البرمجيات، فكتب لنا نصًّا صغيرًا بلغة جافاسكريبت - بالتعبير النمطي (/w+/d{8}) - للمساعدة في أداء وظيفتين: استخلاص أسماء المستخدم للحسابات التي قامت بإعادة التغريد أو الإعجاب بتغريدة محددة، ثم القيام بعملية فلترة سريعة لقائمة أسماء المستخدم بحيث تركز بشكل حصري على أسماء مستخدم ذات سمة معينة، وهي التي تستخدم الاسم متبوعًا برقم من ثماني خانات.

عبْر استخدام هذا النص على إصدار مطوّري البرامج في كروم (Chrome developer tools console)، والذي يوفر لمطوري الويب أدوات مباشرة للاستخدام في المتصفح، وتعمل في الخلفية عند النقر على رابط "إعادات التغريد" أو "الإعجابات" في تغريدة ما، ثم ستظهر النتائج التي تظهر أسماء المستخدم التي تتوافق مع النمط. ويمكنك النقر هنا للاطلاع على النتيجة.

وقد تمكنّا من استخدام هذا النص أيضًا من أجل التحري عن الحسابات التي تتفاعل مع تغريدات لشخصيات بارزة موالية للصين. ففي ذروة الاحتجاجات في هونغ كونغ، نشرت الممثلة الأمريكية من أصل صيني، ليو إيفاي منشورًا على منصة Weibo دعمًا للشرطة في هونغ كونغ، ما دفع البعضَ على شبكات التواصل الاجتماعي إلى إطلاق دعوات لمقاطعة فيلمها الجديد "Mulan". لكنْ قد لاحظنا أيضًا أن العديد من الحسابات على تويتر قد عبّرت عن دعمها للممثلة وفيلمها، وذلك عبر هاشتاغ SupportMulan#.

وقد نشرت سي إن إن تقريرًا حول ذلك. وفكّرنا باستخدام النص (Script)

لتحديد الحسابات التي وضعت إعجابًا على تغريدات مؤيِّدة للفيلم "مولان" أو إعادة التغريدات التي تعبر عن دعمها له.





#SupportMulan Please judge someone after reading words from both sides. Demonstrators're confusing the public by posting some 'truth' and using the hot trend of the movie Mulan. Stop starting a rumour and polish your eyes.



2:58 PM · Aug 16, 2019 · Twitter for iPhone

12 Retweets 111 Likes

ثـم جمعنـا أسـماء الحسـابات التـي تتوافـق مـع النمـط الـذي حددنـاه، ثـم رجعنـا إلـى تواريـخ إنشـائها، لنكتشـف أن معظـم الحسـابات كانـت قـد أنشـئت فـي 16 أغسطس.

https://twitter.com/monicaG62882882	created: 16 August, 20.07h
https://twitter.com/Min85741833	created: 16 August, 05.29h
https://twitter.com/cherry71737735	created: 16 August, 19.22h
https://twitter.com/Catheri57246362	created: 16 August, 06.13h
https://twitter.com/crystal09837022	created: 16 August, 04.16h
https://twitter.com/Suqing26464572	created: 16 August, 06.30h
https://twitter.com/Yates52905656	created: 16 August, 22.16h
https://twitter.com/hu02261927/	created: 16 August, 04.53h
https://twitter.com/xinjin66947005	created: 16 August, 19.18h
https://twitter.com/Ta99869608	created, 16 August, 21.15h

لقد جمعنا تواريخ وأوقات إنشاء هذه الحسابات بشكل دقيق؛ وذلك عبر تمرير المؤشّر على معلومات إنشاء الحساب الخاصة بها، كما يظهر في الصورة أدناه.



وبعد القيام بتحديد هذه الحسابات وجمعها في قائمة واحدة، بدأنا عملية التحليل التقليدية للمحتوى التي كان ينشر عبرها، وسرعان ما اتضح لنا أن الحسابات في هذه القائمة قد نشرت تغريدات تعبّر عن تأييدها للممثلة "إيفاي" وتهاجم المحتجين في هونغ كونغ.



ثم لاحظنا أن الحسابات في هذه القائمة قد تعطلت بعد 17 أو 18 أغسطس، ما يعطي دليلًا آخر على وجود شكل من التنسيق. لا نعرف تحديدًا سبب توقف نشاط هذه الحسابات، ويحتمل أن تويتر قد طلب خطوات إضافية للتحقق من البيانات ولم يتمكن منشئو الحسابات من توفيرها. كما يحتمل أيضًا أنها توقفت عن التغريد حرصًا من أصحابها على عدم إثارة المزيد من الشكوك بشأنها، خاصة في تلك الفترة التي نشطت فيها تويتر في حذف الحسابات الداعمة للصين.

لكن، وبعد عدة أشهر أخرى، لاحظنا عودة نشاط هذه الحسابات، وذلك بهدف نشر محتوى داعم للممثلة إيفاي وفيلمها "مولان".



كما حددنا بعض الحسابات الأخرى الداعمة للفيلم بأنماط أخرى على مستوى اسم المستخدم أو تواريخ الإنشاء، وهي حسابات نشطت بشكل أساسي على نشر تغريدات داعمة للممثلة إيفاي. وقد تتبعنا هذه الحسابات عبر البحث بالوسمين #SuuportMulan أو #Liuyifei.


crystal_28cc @28ccCrystal · Dec 5
cool! #disneyliveaction #SupportMulan
#Liuyifei #CrystalLiu
#mulan #liuyifei #yifei_cc #crystalliu #刘亦菲 #花木兰 #花木蘭 @yifei_cc
Disney @Disney · Dec 5
Loyal. Brave. True. I will bring honor to us all. Watch the brand new trailer for #Mulan. See it in theaters March 27, 2020.
2:06 5.9M views
Your job is to bring
honor to the family...
3


crystal_28cc @28ccCrystal · Aug 16
The real thugs are the demonstrators, not the police.
We support the leading artist of mulan and the Hong Kong police.#Mulan
#LiuYifei #supportmulan
4
18
168


MULAN





Follow
Mulan Our pride.
@kongyuting1
Liu Yifei is a good girl. He has Mulan's qualities of justice and courage and patriotism. He is our pride. Be happy. 刘包子。
Joined August 2019
53 Following 65 Followers





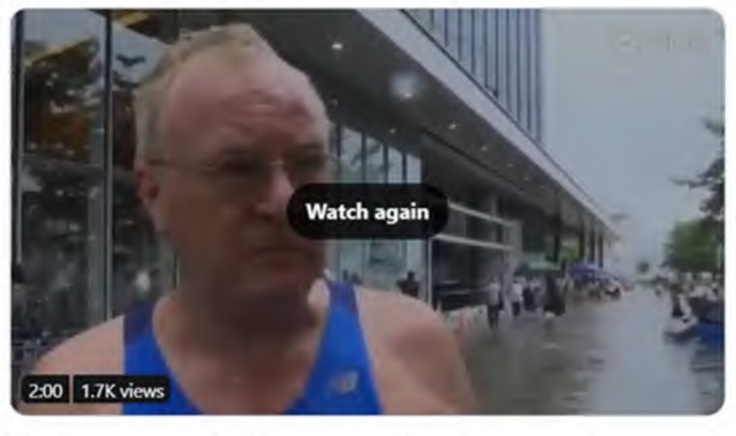
Follow
Cinderlance·icc
@cinderlance
cuz u sucked some
Joined December 2017
48 Following 64 Followers

Mulan Our pride. ❤️ Retweeted



Choco @Choco_Xu · Aug 17

#SupportMulan #Mulan Democracy is not manifested by violence.Why can't people see the truth, she just stands on the side of justice?



18 31 114

Cinderlance-icc Retweeted



Choco @Choco_Xu · Aug 17

#SupportMulan #Mulan Democracy is not manifested by violence.Why can't people see the truth, she just stands on the side of justice?



18 31 114


Mulan Our pride. @kongyuting1 · Sep 25
#mulan #liuyifei #supportmulan #LiuYiFei #花木蘭
十五小甜心 @SNH48_15 · Sep 22
#liuyifei #Mulan Take you to know a real Liu Yifei (Mulan's actor). She always believes in one sentence, the harder she works, luckier she will be. I think one day, people will see the beauty of her bloom.
twitlonger.com/show/n_1sr10p5
3


Cinderlance-icc @cinderlance · Nov 18
#liuyifei so sweet
6
Cinderlance-icc @cinderlance · Sep 18
#LiuYiFei

ويظهـر أن الحسـابات قـد عدَّلـت اسـتراتيجيتها قليـلًا، فتجنّبـت انتقـاد الاحتجاجـات فـي هونـغ كونـغ، وركّـزت بـدل ذلـك علـى الترويـج للممثلـة وفيلمهـا الجديـد، وذلـك ربمـا خوفًـا مـن التعـرض للحـذف مـن قبـل إدارة تويتر.

تظهـر دراسـة الحالـة هـذه إمكانيـة الجمـع بيـن الأسـاليب التقليديـة "اليدويـة" والأسـاليب التقنيـة المؤتمتـة فـي التحقيقـات التـي تسـعى إلـى الكشـف عـن شـبكات الحسـابات المشـبوهة علـى تويتـر. كمـا تُبيّـن أهميـةَ اسـتمرار البحـث عـن المزيـد مـن الحسـابات وأنمـاط النشـاط الرقمـي المشـبوهة حتـى بعـد إعلان أي منصّة عن حذف بعض الحسابات التي تخالف سياساتها.

لقـد اسـتفدنا فـي هـذه العمليـة مـن بعـض أسـاليب البحـث البسـيطة والتحـري عـن تفاصيـل الحسـابات، مـن أجـل تحديـد مجموعـة أكبـر مـن الحسـابات التي يظهر عبر عدد من المؤشرات أنها جزء من حملة زائفة منظَّمة.

الفصل الرابع: التحري عن الفبركات والتلاعب الإعلامي في سياق الأخبار العاجلة

جاين ليتفينينكو

جاين ليتفينينكو صحفية أوكرانية من كييف، تعيش حاليًا في تورونتو الكندية، وتعمل لصالح موقع "باز فيد نيوز" (Buzz-Feed News)؛ حيث تهتم بشكل خاص بحملات المعلومات المضللة، والأمن السيبراني، والتحقيقات الرقمية. كشفت جاين عن العديد من حالات التلاعب الإعلامي على وسائل التواصل الاجتماعي، وعمليات الاحتيال بالعملة الرقْمية، وحملات التضليل الإعلامي التي تسعى لتحقيق الكسب المادي. تسهم جاين في عمليات التحقق من المعلومات للصالح العام في أوقات الأزمات.

بعضُ الأخبار العاجلة -حين تطرأ- تحتاج ساعاتٍ على الأقل أو عدة أيام أحيانًا قبل أن يستوعب المراسلون والمسؤولون حقيقةَ ما حدثَ وتفاصيله وملابساته الدقيقة. ومع بدء تدفُّق بعض المعلومات الأولية والأدلة عبر وسائل التواصل الاجتماعي والمنصات الرقمية، تسنح الفرصة للأطراف ذوي المقاصد الخبيثة لخلق حالة من الانقسام أو التخوين، أو حتى تحقيق استفادة مالية سريعة باستغلال حالة القلق لدى مستهلكي الأخبار، والذين قد يساهمون من جانبهم -وبدون قصد- بنشر المعلومات المغلوطة أو المضللة.

هذه الحالة التي يختلط فيها الفضول الشديد لمعرفة المزيد من المعلومات مع التدفق البطيء للأخبار في الدقائق أو الساعات الأولى لأي حدث هام، تحتّم على الصحفيين أن يكونوا قادرين على المراقبة والتحقق بشكل

فعال من الأخبار الواردة إضافة إلى دورهم أيضًا، لو استدعت الضرورة، إلى دحض أي معلومات غير دقيقة أو مفبركة، سواء كانت تغريدة أم صورة أم مقالًا. فمن المعروف أن المحتوى المزيف لا يحتاج سوى بضع دقائق لصناعته، أما الوصول إلى المعلومات الحقيقية فيتطلب وقتًا أطول.

ومن أهم متطلبات المراقبة والدحض في سياق الأخبار العاجلة هو أن يقف الصحفي على أرضية صلبة، عبر امتلاك المهارات الأساسية في التحقق، كما هو موضّح في دليل التحقّق الأول، وفهم كيفية مراقبة شبكات التواصل الاجتماعي والمنصات الرقمية، ومعرفة الطريقة المثلى للاستجابة في حال تعرَّض الصحفيُّ أو زملاؤه إلى الاستهداف من قِبل أطراف مضلِّلة. هذا يعني أنه لا يسع الصحفيين أن يتعاملوا باستخفاف فيما يتعلق بأمنهم الرقمي.

الخطوة الأولى التي يلزم اتخاذها في حالة الخبر العاجل هي تحديد الجماعة الأساسية المعنيّة بالحادثة. خلال حادثة إطلاق النار في مدرسة ثانوية في مدينة بارك لاند في فلوريدا الأمريكية عام 2018، حصل المراسلون على خريطة "سناب شات" لمقاطع فيديو تبث ما كان يحصل للطلبة العالقين في الغرف الصفية. لكن أثناء إعصار "إيرما" عام 2017، كان التركيز الأكبر على فيسبوك، حيث اعتمد السكّان على المنصّة بشكل أساسي للحصول على المعلومات. لذلك فإنه من الضروري فهْمُ الطريقة التي تعمل بها كلُّ منصة من منصات التواصل الاجتماعي، وكيفيةِ تعاطيها مع أي حادثة.

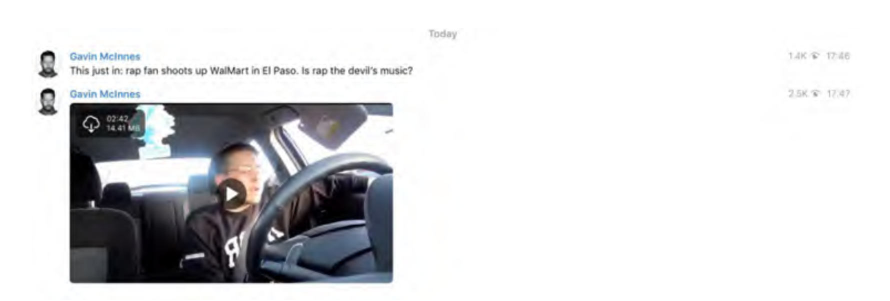
يسلط هذا الفصل الضوء على الأدوات التي يمكن للصحفي استخدامها لمراقبةِ الأخبار العاجلة وكشْفِ الزائف منها. وغنيٌّ عن القول: إنّ كل موقف قد يتطلب أدوات مختلفة، فليس ثمة أداة واحدة تكون هي الأنسبَ لجميع المواقف؛ لذلك فإن تحديد الأطراف المعنية بأي حادثة سيساعد على تحديد الوجهة التي يجب التركيز عليها.

ثلاثة يجب البحث عنها

في ظل سعي المنصات والصحفيين لمحاربة المعلومات المضللة، فإن الأطراف التي تتعمّد نشرها حرصت على تطوير أساليبها كي تتجنب كشفها. ومع ذلك ما يزال من الشائع تحديد بعض الأنماط المتكررة من المحتوى والسلوك الرقمي التي تثير الريبة.

1. الصور المفبركة أو المنشورة في غير سياقها

الجميع يذكر صورة سمكة القرش وهي تسبح أثناء فيضان مياه الأمطار في أحد الشوارع، وهي صورة انتشرت قبل سنوات وما يزال البعض يظن أنها حقيقية حتى اليوم (كانت هذه الصورة موضوعًا لدراسة حالة في دليل التحقق الأول من هذه السلسلة). مثل هذه الصور ومقاطع الفيديو التي ما تزال متداولة رغم اكتشاف زيفها هي ما يطلق عليه العاملون في مجال التحقق وكشف الأخبار الزائفة "تزييفات بسبع أرواح". فالمواد البصرية تنتشر بسرعة أكبر عبر المنصات الرقمية مقارنة بالنصوص، لذا فإن التركيز عليها سيعطي نتائج مثمرة.



خلال حادثة إطلاق النار في مركز "وول مارت" للتسوق في إل باسو عام 2019، حاولت بعض الشخصيات المحسوبة على اليمين المتطرف أن تسيء توظيف مقطع فيديو قديم على يوتيوب غير متعلق بالحادثة.

2. الخطأ في تحديد الضحايا أو الجناة

في أثناء حادثة إطلاق النار في مقر شركة يوتيوب، عجّت وسائل التواصل الاجتماعي بالادعاءات المغلوطة بشأن المتورطين في الجريمة.

وخـلال فتـرة الانتخابـات النصفيـة فـي الولايـات المتحـدة عام 2018، انتشـرت شـائعات بشـأن مشـاركة مهاجريـن غيـر قانونييـن فـي التصويـت، بحسـب مـا ادّعـى الرئيـس الأمريكـي نفسـه. علينـا إذن أن نتنبـه إلـى أنـه كثيـرًا مـا يسـتغلّ البعض سياق الأخبار العاجلة لتوجيه الاتهامات زورًا إلى أطراف بريئة.



فـي حـادثـة إطـلاق النـار في بـارك لانـد عـام 2018، حـاول حسـاب مزيَّـف باسـم بيـل أوريلـي نشْـرَ اسـم غيـر صحيـح للمشـتبَه بـه.

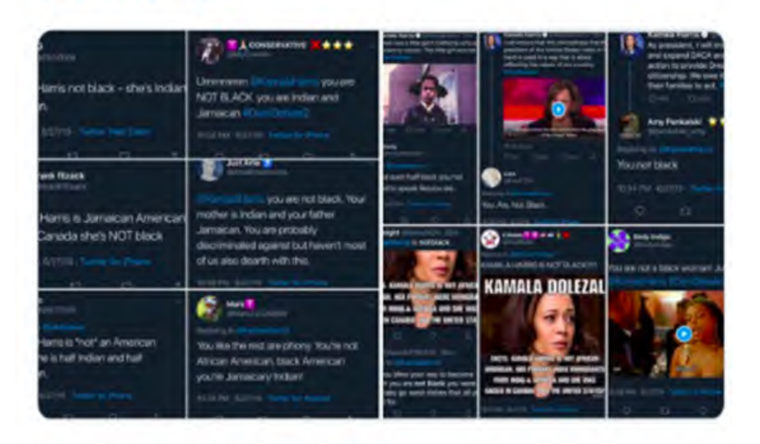
3. الحمَلات المنسَّقة والاستهداف الإلكتروني

قـد لا ينـدرج هـذا تحـت المعلومـات المضلِّلـة، إلا أن بعـض الأطراف المسيئة تلجـأ عـادة إلـى التحـرش والإسـاءة إلـى الأشـخاص المعنييـن بقضيـة مـا كوسيلة لإسـكاتهم. وقـد يكـون ذلـك أيضـًا إشـارة إلـى أن جهـة مـا أو مجموعة مـن الأشـخاص يتابعـون موضوعـًا أو حدثـًا معينـًا، وقـد يلجؤون إلـى تكتيكات

مختلفة حسبما تقتضي التطورات. أما حملات التضليل الجماعية الموجَّهة (Brigading)، فتحصل حين يقوم مجموعة من الأشخاص بالعمل معًا من أجل خلق صورة وهميّة بوجود قاعدة واسعة من التفاعل أو ردّات الفعل على قضية ما، وذلك عبر تصعيد محتوى ما أو تهميشه أو إغراق مستخدم ما بالتعليقات على محتوى معين يقوم بنشره.



A lot of suspect accounts are pushing the "Kamala Harris is not Black" narrative tonight. It's everywhere and it has all the signs of being a coordinated/artificial operation. #DemDebate2



12:22 AM · Jun 28, 2019 · Twitter for iPhone

5.5K Retweets 9.6K Likes

بعد مناظرة بين مرشحين عن الحزب الديمقراطي عام 2019، عمدت حسابات مجهولة إلى نشر رسائل موحّدة تتحدث عن عرق كامالا هاريس.

أفضل الممارسات للأرشفة والنشر

من الضروري قبل الشروع في الكشف عن الفبركات أن يكون لديك ملفٌّ يضمّ المستندات المتوفرة لديك، وأن تنشئ جدولًا (Spreadsheet) تُدرِج فيه كلَّ ما تعثر عليه. قم على الفور بالتقاط صور للشاشة (Screenshot) لكلِّ فبركة تعثر عليها أو أي محتوى تكتشفه، وقم بأرشفة الصفحة التي وجدت فيها هذا المحتوى. ويمكنك الاستفادة من الإضافة الخاصة بالمتصفح (Extension) التي يوفرها موقع Archive.org، وهي أداة مجانية وسريعة وفعالة لأرشفة المحتوى. احرص أيضًا على تدوين الروابط الأصلية والمؤرشفة للمحتوى في الجدول الذي لديك. ستساعدك هذه الخطوات على استعادة ما عثرت عليه والتحري عن أي أنماط مشتركة مشبوهة.

ولتفادي المشاركة في انتشار الصفحات المرتبطة بالمعلومات المغلوطة أو المضلِّلة، احرص على الاعتماد على الرابط (URL) المؤرشَف لأي مقالات أو منشورات على وسائل التواصل الاجتماعي وليس الرابط الأصلي.

من الممارسات المعتمدة كذلك وضع إشارة مائية (Watermark) على الصور ودمغها بأنها "زائفة" أو "مضللة" لضمان ألّا تُستخدم الصور في خارج سياقها.

وفي حال كتابة مقال، فعليك التركيزُ في العنوان والنص على ما هو حقيقي، بدل الاكتفاء بالإشارة إلى ما هو زائف وإعادة تدويره بطريقة غير مقصودة؛ فقد أثبتت الدراسات أن تكرار المعلومات الزائفة قد يؤدي بالناس إلى استبطانها وحِفظها، لذا يجدر بالصحفي أن يتجنب تكرار مثل هذه المعلومات والفبركات وألّا يذكرها إلا بالحدّ الأدنى، وعليك توجيهُ تركيز العامة نحو المعلومات الدقيقة.

تحديد الكلمات المفتاحية والمواقع

عند ورود أخبار عاجلة تتعلق بحادثة ما، قم بوضع قائمة من المواقع (Loca-tions) والكلمات المفتاحية ذات العلاقة.

على مستوى الموقع، عليك أن تحدد (المدينة، والولاية، والدولة...) وأي معلومات أخرى تتعلق بالموقع؛ مثل: الاسم المشهور للمدينة أو الحيّ الذي وقعت فيه الحادثة موضوعُ الخبر العاجل. عليك في سياق الانتخابات مثلًا أن تحرص على امتلاك معرفة دقيقة حول المنطقة أو الدائرة الانتخابية المعنية واسمها وبعض التفاصيل الخاصة بها؛ فمِن شأن هذه المعلومات أن تساعدك على الوصول إلى المنشورات المحدّدة بالموقع الجغرافي، إضافة إلى البحث عن أي منشورات تضمنت ذكر هذا الموقع.

احرص أيضًا على الوصول إلى حسابات التواصل الاجتماعي لأي جهة رسمية محلية معنية، ومتابعة منشوراتها، مثل أقسام الشرطة أو الإطفاء، إضافة إلى الشخصيات السياسية والإدارية ووسائل الإعلام المحلية.

تأتي بعد ذلك مهمة تحديد الكلمات المفتاحية، ويتضمن ذلك مثلًا كلمات مثل "ضحايا"، "قاتل"، "مشتبه به"، "إطلاق نار"، "حريق"، "فيضان"، "انفجار"، أو أسماء أشخاص تأكدَت علاقتهم بالحادثة، أو حتى عبارات عامة مثل "البحث عن...". من المهم أيضًا التفكير في العبارات التي قد يستخدمها الناس مع مثل هذه الأخبار بالإضافة إلى الكلمات المفتاحية. وفي حال لاحظتَ وجود حساب يبدو أنه موثوق ويقول بأنه موجود في مكان الحدث، فعليك الاهتمام جيدًا بمتابعة هذا الحساب وقراءة تغريداته كاملة. كما قد تستفيد من البحث في قائمة متابعيه أو أصدقائه لعلك تجد المزيد من الحسابات التي يكون أصحابها موجودين في المكان أو يكونون من بين المتأثرين بالحادثة.

لاحِظ أنه وفي سياق الحوادث التي تثير الفزع أو القلق قد يتسرع الناس في كتابة أسماء الأماكن. ففي حريق حصل عام 2019 في منطقة كنكايد (Kin-cade) في كاليفورنيا، بدأ الناس باستخدام وسم #kinkaidfire، وذلك

غالبًا بسبب تقنية تعديل الكتابة الآلية. لذلك فكّر بالبحث عن الموقع بالتهجئات الخاطئة الممكنة، وانظر النتائج التي يمكن أن تحصل عليها.



من المهم كذلك محاولة التواصل مع أيّ من المصادر التي تعرفها والتي قد تُوجَد في ذلك الموقع، أو تنتمي للمجتمع الذي قد يكون مستهدَفًا في حملة التضليل أو التشويه، واسألْهم عن رأيهم فيما يُنشر على الإنترنت. يمكنك أن تخبر متابعيك بأنك ترغب في التحقق إن كان ثمة عملية تضليل بالمعلومات أو غير ذلك من أشكال المحتوى الإشكالي المتعلق بخبر أو حدث ما. حاوِل التنسيق مع فريق شبكات التواصل التابع للمؤسسة التي تعمل بها؛ للمساعدة في نشر طلبك المتعلق بتوفير المعلومات من الموقع موضوع التحرّي.

أدوات أساسية للتعامل مع الصور

1. البحث باستخدام الصور

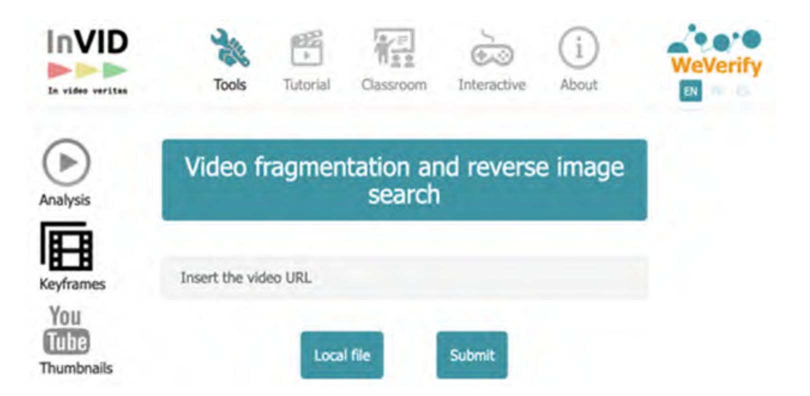
يعد البحث العكسي باستخدام الصور من أهم الطرائق للتحقق من صورة ما والحصول على مزيد من المعلومات عنها. يمكن البحث عن صورة ما على محرك البحث جوجل، عبر النقر بيمين الفأرة على الصورة، واختيار "البحث في جوجل عن الصورة" (Search Google for Image).

لكن هذا لا يُغني عن التحري عن الصورة باستخدام أدوات أخرى. يمكن إضافة ملحق (InVID) على محرك البحث والتي تساعد على البحث عن الصور عبر عدّة أدوات. يوضح الجدول التالي الذي أنجزه موقع Domain Tools أوجُهَ التميّز والضعف في عدد من الأدوات الخاصة بالتحري عن الصور.

	Elements Identified	Faces	Structures	Places	Digital/ Logos	Alternate Sizes	Flipped or Altered
Google	1	Neutral	Great	Great	Great	Good	Neutral
Yandex	2+	Great	Great	Great	Good	Good	Good
Bing	3+	Good	Good	Good	Good	Neutral	Great
TinEye	1	Neutral	Neutral	Neutral	Great	Great	Good

InVID

إحدى الإضافات المجانية (Extension) على محرك البحث، ومن أهم الأدوات لتحليل مقاطع الفيديو والتحقق منها. تساعد هذه الأداة المستخدِم على البحث عبر رابط الفيديو، بحيث تعمل على سحب صور مقتطعة "ثمبنيل" من الفيديو، لاستخدامها بأدوات البحث العكسي عبر الصور وتحديد أين ظهر مقطع الفيديو سابقًا على الإنترنت.



2. البحث في TweetDeck

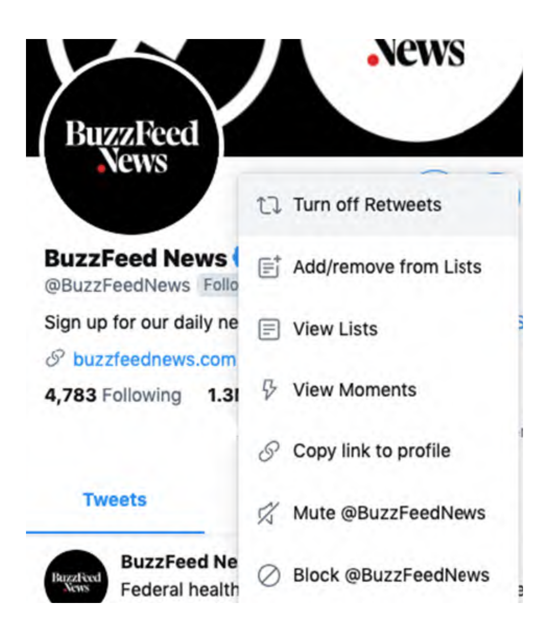
تعدّ منصّة "تويت ديك" إحدى أفضل الطرائق للبحث في تويتر؛ لأنها تتيح للمستخدم إنشاء أعمدة خاصة بعمليات البحث والقوائم. فالعثور على القوائم ذات العلاقة ونسخها عملٌ أساسيّ من أجل الاطلاع بشكل مستمر على وضع ما.

يمكن البحث عبر جوجل على قوائم تويتر باستخدام صيغة بسيطة: اكتب على محرك البحث: twitter.com/*/lists، ثم ضع الكلمة المفتاحية بين علامتي تنصيص. فلو كنا نبحث مثلًا عن مراسلين في ولاية ألاباما، فيمكن أن نكتب:

“site:twitter.com//lists “Alabama reporters*

وستظهر لنا في نتائج البحث أيّ قوائم أنشأها مستخدمون في تويتر، وتشتمل في عنوانها على عبارة "Alabama Reporters".

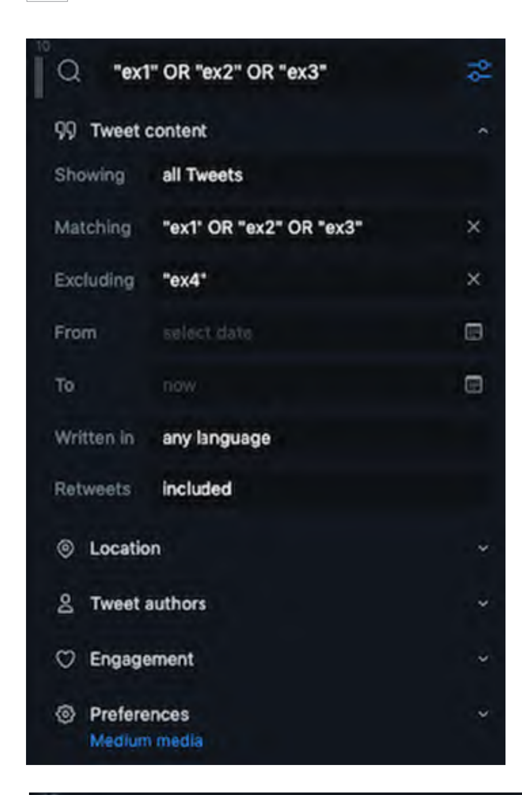
عند العثور على القائمة المطلوبة والمفيدة لموضوعك، ستحتاج إلى نسخها لإضافتها إلى منصة "تويت ديك". ويمكنك الاستفادة من هذا التطبيق لنسخ القوائم التي تريدها، وهي طريقة أفضل من مجرد الاكتفاء بمتابعة القائمة، وذلك لأن نسخها يتيح لك إضافة أو حذف المستخدمين منها.



قد يكون من الضروري -إضافةً إلى العثور على القوائم وإضافتها إلى "تويت ديك"- أن تقوم بإنشاء أعمدة تشتمل على فلاتر بحث خاصة تمكِّن من التحري السريع عن الكلمات المفتاحية والصور ومقاطع الفيديو. يلزمك من أجل البحث عن عدّة كلمات مفتاحية أن تحيطها بعلامات تنصيص وأن تضع "OR" بينها، مثل:

“Kincade” OR “Kinkade.”.

يمكنك كذلك استثناء كلمات محددة من البحث إن كان استخدامها سيؤدي إلى ظهور نتائج غير مطلوبة. معظم الناس حاليًّا لا يحددون الموقع في التغريدات، لذا يمكن أن تترك هذا الحقل فارغًا أثناء البحث؛ كي تصل إلى أكبر قدْر ممكن من النتائج.


"ex1" OR "ex2" OR "ex3"
Tweet content
Showing
all Tweets
Matching
"ex1" OR "ex2" OR "ex3"
Excluding
"ex4"
From
select date
To
now
Written in
any language
Retweets
included
Location
Tweet authors
Engagement
Preferences
Medium media


"ex1" OR "ex2" OR "ex3"
Tweet content
Matching '"ex1" OR "ex2" OR "ex3"', excluding '"ex4"'
Location
Tweet authors
Engagement
At least 1 Retweets
at least 1 likes
and at least 0 replies
Preferences
Medium media
Share
Clear
Remove

وإن كنت ترغب في فلترة النتائج بشكل أدقّ، فحدِّد التاريخ في خانة "From" ليكون قبل يوم أو يومين من الحدث، وذلك للتأكُّد من الاطلاع على أي تغريدة محتمَلة قد تمَّ نشرُها من منطقة زمنية مختلفة.

وبإمكانك في حالة الحصول على حجم كبير جدًّا من النتائج وتصفيتها عبر عامل "التفاعل"، وذلك كي تضمن الحصول على التغريدات التي نالت قدرًا كبيرًا من الإعجابات أو إعادات التغريد.

ويمكنك أيضا البحث التفصيلي عن كل جزء من العبارة المفتاحية، بوضع كلّ منها في عمود منفصل؛ فيمكن مثلًا وضعُ "الموقع" (loca-tion) في أحد الأعمدة، والكلمات المفتاحية الأخرى في عمود آخر. وعادة ما أقوم بالبحث عبر عمود ثالث وأكتب فيه أسماء بعض المشتبَه بهم أو الضحايا، مع الأخذ بالاعتبار للتهجئة الخاطئة المحتمَلة للأسماء.

وأخيرًا، إن كانت عملية البحث تُنتج قدرًا أكبر من اللازم من النتائج، فيُنصح بإنشاء عمود جديد؛ لتَبحث عبره عن الكلمة المفتاحية الأفضل، وتعرض نتائج البحث عبر فلتر "Tweet Content" والذي يُظهر التغريدات التي تتضمن الصور ومقاطع الفيديو فقط، وهكذا تحصل على نتائج تساعدك على تحديد ما إذا كان هنالك أيّ محتوى بصري مفيد.

3. CrowdTangle

تطبيق على الويب وإضافة على المتصفح يمكن الاستفادة منه بشكل مجاني في غرف الأخبار (يمكنك التواصل مع الشركة إن لم يكن لغرفة الأخبار التي تعمل لصالحها حساب يتيح الاستفادة من الأداة).

تتيح لك هذه الأداة إنشاء لوحات تحكم (Dashboards) لمراقبة المحتوى عبر فيسبوك وإنستغرام وريديت. يمكنك أيضًا البحث عبر الكلمة المفتاحية وفلترة النتائج عبر عدة عناصر، مثل وقت النشر، واللغة، ومستوى التفاعل.

ولهذه الأداة أهمية خاصة إن كنت مهتمًا بمراقبة المحتوى على فيسبوك، والبحثِ عن رابط ما، وأين تمّ نشره على المنصة وغيرها من المنصات.

عند الحصول على حساب على الأداة، اذهب إلى الموقع الخاص بالتطبيق لتسجيل الدخول وإنشاء "لوحة تحكم" جديدة. أما في حال لم يكن لديك حساب؛ فبوسعك الاستفادة من الإضافة المجانية (Extension) الخاصة بالمتصفح.

البحث عن منشورات في فيسبوك عبر "كراود تانغل"

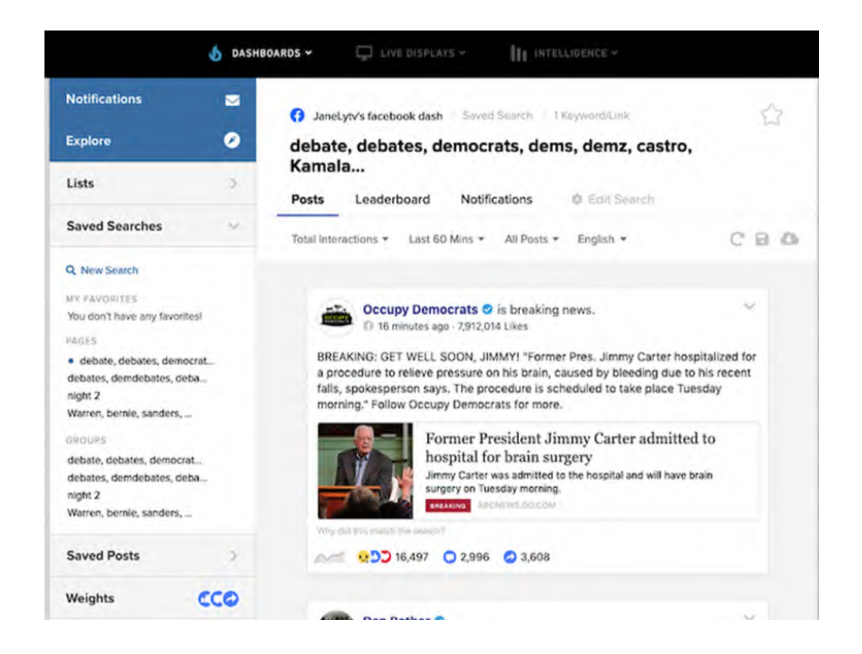
اضغط على "عمليات البحث المحفوظة" (Saved Searches) على الشريط الجانبي الأيسر، ثم انقر على "New Search". ثمة خياران للبحث في فيسبوك: البحث في الصفحات أو البحث في المجموعات، وأنا أفضّل البحث فيهما معًا.

يمكنك البحث باستخدام ما يتوفر لديك من كلمات مفتاحية، واستخدام فاصلة بين كلمة وأخرى. يمكنك أيضًا تحديد عرض المنشورات، سواء باختيار التغريدات الأحدث، أم الأكثر رواجًا، أم ذات النشاط الأعلى نسبيًا (Overperforming)، أي المنشورات التي تتلقى قدْرًا من التفاعل أعلى من العادة في صفحة ما، وعادة ما أختار الطريقة المناسبة بعد تقدير الموقف؛ للتأكد من الوصول إلى المحتوى الرائج والجديد.

يمكن أيضًا فلترة المنشورات للبحث ضمن إطار زمني أو نوع محدد. وقد أتاح "CrowdTangle" مؤخرًا إمكانية البحث في المنشورات عبر موقع الصفحة التي نشرت بها. فعند الضغط على خيار اللغة "English"، والدولة "Country"، يمكنك أن تختار المنشورات التي ظهرت في صفحات موقعها المحدد عند إنشائها هو الولايات المتحدة مثلًا. يمكن أيضًا البحث عن منشورات في صفحات من إيران أو

روسيا أو السعودية أو الفلبين أو الهند أو غيرها. ومن المهمّ الانتباه بشكل خاص إلى المنشورات التي تتضمن صورًا أو مقاطع فيديو، وذلك لأنها عادة ما تنتشر بشكل أسرع وتحقق تفاعلا عاليا من المستخدمين.

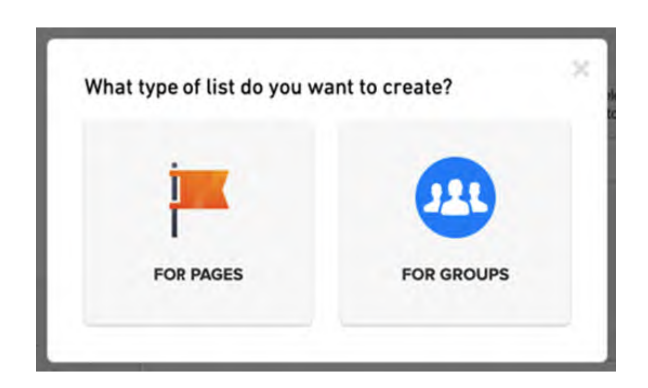
عند تحديدك لعناصر البحث المطلوبة والحصول على النتائج ذات العلاقة تأكد من حفظ العملية؛ كي تتمكن من العودة إليها لاحقًا للاطلاع على المزيد من النتائج والتنقيب فيها.



القوائم في كراود تانغل

تتيح أداة "Crowdtangle"، كما في موقع TweetDeck، إنشاء قوائم بالصفحات والمجموعات العامة التي تهتم بمتابعتها. عند الضغط على "قوائم" (Lists) على الشريط الجانبي ثم "إنشاء قائمة" (Create List)، ستكون قادرًا على مراقبة الصفحات أو المجموعات بحسب الكلمات المفتاحية التي قمت باختيارها أو الصفحات التي وضعت روابطها. كما يتوفر في أداة "كراود تانغل" نفسها عدد من القوائم الجاهزة التي يمكن الاستفادة منها عبر

الضغط على "Explore". وكما هي الحال في تويتر، فإن إنشاء القوائم التي تضم صفحات أو مجموعات تتحدث عن الموضوع أو الحدث الذي تتحرى عنه سيكون وسيلة ناجعة لمراقبة المعلومات والبيئات التي تنتشر بها.



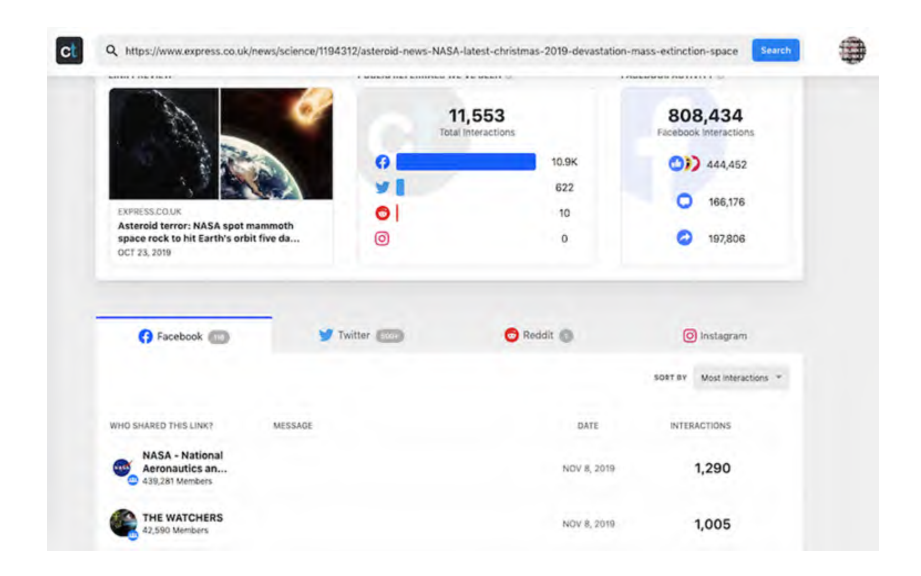
البحث عبر الرابط في كراود تانغل

يمكن كذلك الاستفادة من "كراود تانغل" في عمليات البحث عبر الرابط. توجّه إلى https://apps.crowdtangle.com/search/ وضع الرابط أو الكلمات المفتاحية للمحتوى الذي تبحث عنه، وستظهر لك عبر كراود تانغل أبرز الحسابات التي قامت بمشاركة الرابط على فيسبوك وإنستغرام وريديت وتويتر (لكن النتيجة في تويتر ستكون مقتصرة على آخر سبعة أيام).

وسيساعدك ذلك على تحديد كيفية انتشار محتوى ما، وما إذا كان ثمة مجموعات أو حسابات قد يلزم التحرّي عنها بشكل أعمق، إضافة إلى تحديد ما إذا كان محتوى ما قد انتشر بشكل يستدعي أن يتدخل الصحفيّ من أجل بيان زيفه إن كان زائفًا.

وتجدر الإشارة هنا إلى عدم وجود قواعد ثابتة لتقرير ما إذا كان من اللازم دحض محتوى مزيف ما، لكن يمكن الاستئناس عمومًا بهذه الأسئلة: هل انتشر المحتوى خارج الشبكة الأولية للحسابات التي شاركته؟ هل شارك المحتوى شخصيات عامة تمثل سلطة ما؟ هل أثار قدرًا ضخمًا من التفاعل؟ (الإضافة المجانية على المتصفح تقدم نفس

النتائج فيما يتعلق بالبحث عبر الرابط، وهي عملية مجانية على الإضافة وعلى تطبيق الويب دون الحاجة إلى وجود حساب على كراود تانغل).



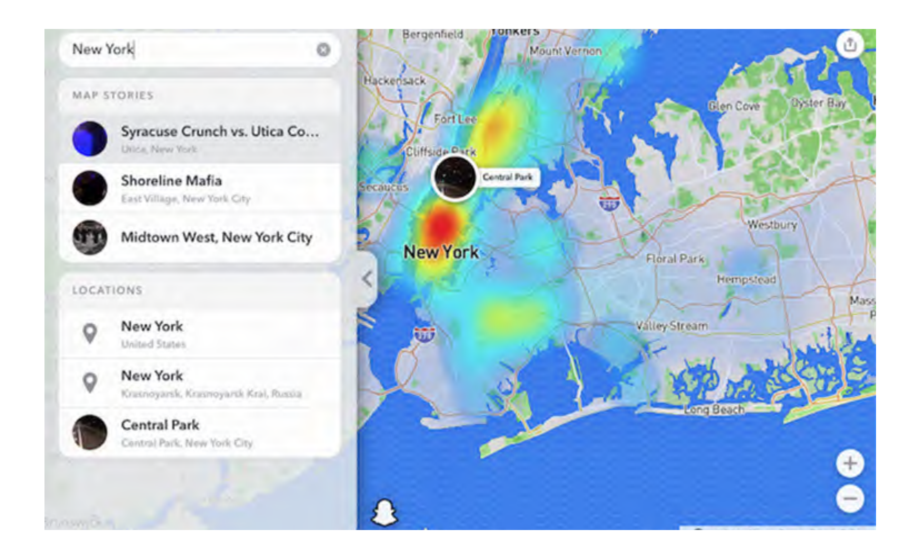
4. البحث في إنستغرام

إنستغرام منصة مهمة للبحث عبر الوسوم والمنشورات المحددة بموقع جغرافي. يمكن البحث عبر المواقع ذات العلاقة، وتذكّر أن الموقع يمكن أن يشير إلى حيّ أو مَعْلَم ما. وفي حال عثورك على شخص ما يَظهر أنه متابع لخبر أو حادث ما، توجّهْ إلى حسابه واحرص على متابعة القصص (Stories) التي نشرها، فالقصص على إنستغرام تحظى بمتابعة أكبر مقارنة بالمنشورات العادية. تصفح كذلك التعليقات على بعض المنشورات ذات العلاقة، إذ يمكن أن تجد من بينها تعليقات لشهود عيان محتملين، كما أنه من الضروري أيضًا ملاحظة أي وسوم جديدة ذات علاقة بالقصة التي تبحث عنها. إن كنت تريد أرشفة قصة إنستغرام ظهرت على حساب ما، فيمكن الاستفادة من موقع storysaver.net لتنزيل القصة وحفظها.

5. سناب ماب

لا تنتشر المعلومات المضللة كثيرًا على "سناب شات"، لكن الخريطة العامة على هذا التطبيق مفيدة للتحقق من أي محتوى أو الكشف أنه زائف. اذهب

إلـى موقـع map.snapshat.com وابحـث عبـر الموقـع المطلـوب، وسـتحصل علـى خريطـة حراريـة (Heat map) توضح مكان نشـر المحتوى، ويـدل تركـز اللـون علـى أن المنطقـة تشـهد نشـاطًا أكبـر علـى التطبيـق. ولحفـظ سـناب مفيـد، اضغـط علـى النقـاط الثلاثـة أعلـى اليمين، ثم قـم باختيار "مشـاركة" (Share)، ثـم انسـخ الرابـط للاطـلاع عليـه لاحقًـا، ولا تنـس بالإضافـة إلى ذلك حفظ صور مقتطعة للشاشة (Screenshots) للسناب المطلوب.



الاستفادة من البيانات والتوصل إلى النتائج

مـن الضـروري جـدًا التـدرّب علـى ممارسـة كل واحـدة مـن هـذه الأدوات لتحقيـق الاسـتفادة المرجـوّة منهـا عنـد حـدوث أخبـار عاجلـة. تذكّـر أن المعلومـات المضللـة تتقن اللعـب علـى العواطـف واسـتغلال الفجـوات التـي تحصـل أثنـاء التغطيـات الإخباريـة، ومـن المهـم أن يكـون ذلـك فـي الحسـبان أثنـاء البحـث علـى الإنترنـت. مـن الـوارد رغـم ذلـك أن تجد بعـض المعلومات الدقيقـة التـي تسـاعدك وتسـاعد زمـلاءك فـي غرفـة الأخبـار. دوّن كل المعلومـات التـي تعتقـد أنهـا دقيقـة، لتسـهّل مهمّـة مقارنتهـا بالمعلومـات الجديـدة التـي تشـكّ فـي صحتهـا، ولا تتـردّد فـي طلـب المسـاعدة مـن أي زميل من مؤسستك في الميدان.

وبعد هدوء حالة الانفعال المتزامنة مع الحوادث والأخبار العاجلة، سيكون من الجيد أن تنظر من جديد إلى الصور والمنشورات التي قمت بحفظها. ففي حين يتركز اهتمامنا أثناء تدفق الأخبار العاجلة والجلبة المصاحبة لها على توضيح الأخبار والمعلومات الزائفة وغير الدقيقة كلما ظهرت -وذلك كجزء من مسؤوليتنا الصحفية تجاه العامة- فإن الاهتمام يجب أن ينصبّ بعد أن تهدأ العاصفة على النظر إلى التفاصيل التي قمنا بجمعها في إطارها الأوسع؛ سعيًا لاكتشاف أية أنماط أو اتجاهات عامة بخصوص الفبركات أو المعلومات المضللة والحسابات التي قامت بنشرها.

فعلينا أن نسأل مثلًا إن كان هنالك استهداف لعرق أو جندر ما، وهل الفبركات التي صدرت من حسابات صغيرة ومغمورة حققت رواجًا واسع النطاق؟ هل كان أداء إحدى منصات التواصل الاجتماعي متميزًا عن الشركات الأخرى سلبًا أو إيجابًا؟

من الممكن أيضًا لكتابة تعليق مطوّل حول العمليات التي أجريتها أن تساعد القرّاء على أن يفهموا بشكل أفضل الغاية من حملات التضليل والأساليب التي تتبعها تلك الحملات، كما يمكن أن يكون ذلك أداة بحثية مفيدة لك شخصيًّا أو لزملائك في غرفة الأخبار، لتحديد الجوانب التي قد يلزم التركيز عليها بشكل أفضل في مواقف مماثلة في المستقبل.

الفصل الخامس: التحقق من الصور ومساءلتها

هانا غاي، فريدة فيس، سيمون فوكنر

فريدة فيز هي مديرة مختبر المحتوى البصري على وسائل التواصل الاجتماعي، وهي أستاذة الإعلام الرقمي في جامعة مانشستر المتروبوليتانية. تهتم فريدة في عملها الأكاديمي والصحفي بظاهرة تفشي المعلومات الزائفة على الإنترنت. كانت عضوًا في مجلس الأجندة العالمية لشؤون وسائل التواصل الاجتماعي التابع للمنتدى الاقتصادي العالمي (2013-2016)، وهي حاليًّا مديرة مؤسسة "Open Data Manchester".

سيمون فوكنر محاضر في تاريخ الفن والثقافة البصرية في جامعة مانشستر المتروبوليتانية، وتهتم أبحاثه بدارسة التوظيف السياسي للصور ومعانيها السياسية، مع تركيز خاص على النشاط الحقوقي والحركات الاحتجاجية. يشغل سيمون أيضًا منصب المدير المشارك لمختبر العناصر البصرية في وسائل التواصل الاجتماعي، وهو معني بشكل خاص في تطوير الطرق التي تساعد على تحليل الصور التي تحظى بالرواج على وسائل التواصل الاجتماعي.

هانا غاي باحثة في مرحلة الدكتوراه في جامعة مانشستر المتروبوليتانية، تهتم بتوضيح دور الصور في نشر المعلومات المضللة على وسائل التواصل الاجتماعي. غاي عضو في مختبر العناصر البصرية في وسائل التواصل الاجتماعي، وتتابع حاليًا بعض المشاريع التي تتحرى عن مجموعة من الصور التي انتشرت

على تويتر أثناء حراك "حياة السود مهمّة" في الولايات المتحدة، إضافة إلى المشاركة في حملات توعية في المدارس الكندية بكيفية التعاطي مع عناصر الإعلام البصرية من أجل محاربة انتشار المعلومات الزائفة.

للمواد البصرية في وسائل التواصل الاجتماعي نصيب الأسد من التداول والانتشار، فالصور ومقاطع الفيديو أكثر تأثيرًا وإقناعًا ولفتا للانتباه وإثارة للتعاطف، كما أن إنتاج هذه المواد قد بات في غاية السهولة للجميع. والنتيجة هي أن هذه المواد قد باتت وسائل مفضَّلة لعمليات نشر المعلومات الزائفة والمضلِّلة.

وقد درجت العادة في النقاشات المتعلقة باستخدام المواد البصرية -في سياق حملات المعلومات الزائفة والمضللة- على التركيز إمّا على آليات التحقق وإما على عمليات التحقق من عمليات التزييف العميقة في مقاطع الفيديو، وهو ما بات رائجًا في الآونة الأخيرة. لكن وقبل أن نتناول مسألة الزَيف العميق في الفصل التالي، يلزمنا أولًا أن نتعرف بشكل جيد على الاستخدام غير المعقد تقنيًا للصور والفيديوهات المضللة، خاصة تلك التي تظهر في غير سياقها.

وبالنظر إلى التوظيف الواسع للمواد البصرية في المحاولات الخاصة بالتأثير على الرأي العام والتحكم به، فإن على الصحفيين امتلاك مهارات أساسية في التحقق من الصور، واكتساب القدرة على طرح الأسئلة النقدية المناسبة، وتقييم الصور لفهم كيفية توظيفها وملابسات ذلك. وسنركّز في هذا الفصل على بيان هذه المهارات المطلوبة وتطويرها، عبر اتباع إطار عملٍ طورناه في مختبر العناصر البصرية في وسائل التواصل الاجتماعي (Visual Social Media Lab).

البناء على عمليات التحقق

نركّز في المختبر الخاص بالعناصر البصرية في وسائل التواصل الاجتماعي على فهم الأدوار التي تؤديها الصور التي تنتشر عبر الإنترنت في مجتمعاتنا. وفي حين ينصب تركيزنا بشكل أساسي على الصور الثابتة، فإن هذا لا يُسقط من الاعتبار أهميةَ الأنواع الأخرى من الصور، مثل الصور المركبة، والميمات Memes، والصور البيانية، ولقطات الشاشة (Screenshots)، وغيرها.

ويتطلب التعامل مع المعلومات المضللة والزائفة في المحتوى البصري بعض الاستراتيجيات المحددة؛ وما يزال الانشغال الأساسي بين الصحفيين اليوم فيما يتعلق بالتحقق من الصور منصبًا على تحديد مصداقية ما تنقله الصورة.

وفي دليل التحقق الأول، وضح تروشار باروت أربعة مبادئ أساسية فيما يتعلق بالتحقق من الصور، ومن الضروري الرجوع إليها باستمرار. كما يمكن الاستفادة من دليل التحقق البصري في مؤسسة "فيرست درافت"، والذي يعد مصدرًا مهمًّا يستخدم هذه المبادئ ويطرح خمسة أسئلة فيما يتعلق بالصور ومقاطع الفيديو:

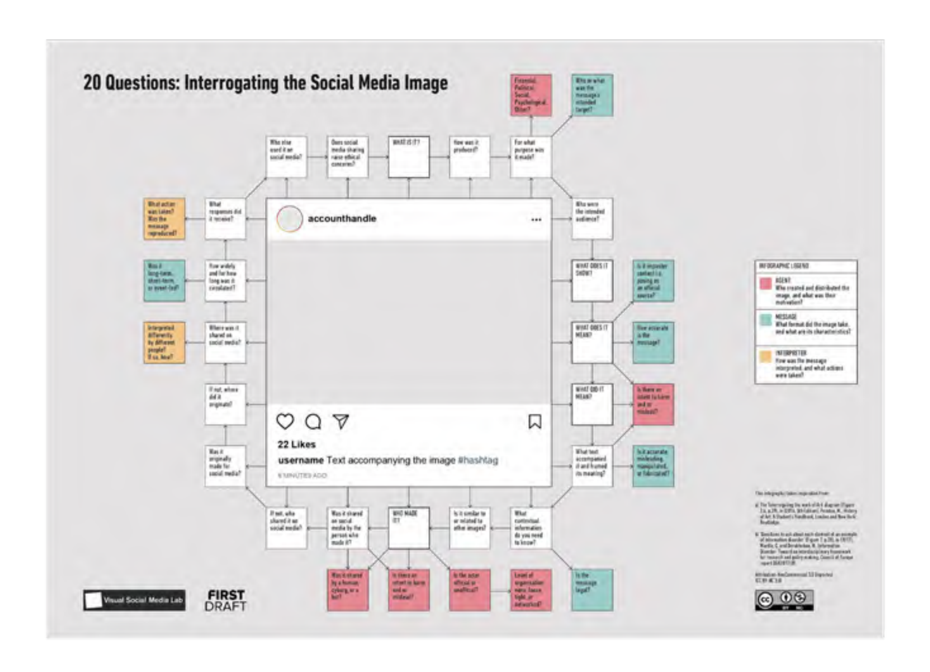
1. هل نحن أمام النسخة الأصلية؟
2. هل تعلم مَن التقط الصورة؟
3. هل تعلم مكان التقاط الصورة؟
4. هل تعلم متى التُقطت الصورة؟
5. هل تعلم سبب التقاط الصورة؟

وثمة العديد من الأدوات المعروفة التي تساعد في التحقق من الصور ومقاطع الفيديو منها InVID، وYandex Image Search، وTin-Eye، وForensically، إضافة إلى خيار البحث عن الصور في جوجل. وتركز هذه الأدوات الخاصة بالتحقق على استبيان المصدر الأصلي لصورة ما.

ورغـم أهميـة هـذه الطريقـة، إلا أن الاسـتراتيجيات والأسـاليب المسـتخدمة عـادة فـي نشـر المعلومـات الزائفـة والمضللـة وحمـلات التضليـل الإعلامـي بأشـكالها المختلفـة، تسـتلزم كذلـك النظـر فـي كيفيـة نشـر الصـور وتوظيفهـا والأطـراف التـي تقوم بذلـك، إضافـة إلـى ملاحظـة الـدور المحتمـل للصحفيين في الترويج للصور الإشكالية.

سـنتجاوز فـي هـذا الفصـل الحديـث عـن الأسـاليب التقليديـة المعروفـة فـي التحقـق مـن الصـور، وسـندمج بعـض الأسـاليب مـن مجـال تاريـخ الفنـون ونقـارب المشـكلة عبـر عـدد مـن الأسـئلة التـي وُضعـت خصيصًـا للتعامـل مـع المحتـوى المزيـف أو المضلـل. هـذه الأسـئلة تشـكِّل الإطـارَ الـذي وضعناه بعنـوان "20 سـؤالًا للتحـري عـن الصـور علـى وسـائل التواصـل الاجتماعي"، وهـو إطـار تـم تطويـره بالتعـاون مـع زملائنـا فـي مؤسسـة "فيرسـت درافت"، ليكون بمثابة أداة إضافية للصحفيين للتحقق من الصور.

التحري عن الصور في وسائل التواصل الاجتماعي



يقوم هذا الإطار على 20 سؤالًا يمكن طرحها أثناء عملية التحقق من أي محتوى بصري أيًّا كان شكله (صورة ثابتة، مقطع فيديو، GIF، إلخ)، على وسائل التواصل الاجتماعي، إضافة إلى 14 سؤالًا إضافيًا لغايات البحث المعمق في الجوانب المتعددة للمحتوى المزيف أو المضلل. هذه الأسئلة لا تتبع ترتيبًا محددًا بالضرورة، ولكن يمكن عمومًا البدء بهذه الأسئلة الأولية الخمسة:

1. ما هي الصورة؟
2. ماذا يظهر فيها؟
3. مَن صاحب الصورة؟
4. ماذا كان الهدف من إنشائها؟
5. ما هدف استخدامها؟

لا تختلف الأسئلة الثلاثة الأولى كثيرًا عن الأساليب المعروفة المتَّبعة في التحقق من المحتوى البصري، وتحديد نوعه (صورة، فيديو، إلخ) وماذا يظهر فيها ومن أنشأها.

أما السؤالان الرابع والخامس فيتعاملان مع اعتبارات أخرى للمعنى الذي يتضمّنه هذا المحتوى والمعنى الذي وُظّف لخدمته، والذي قد يكون مفارقًا للمعنى الأصلي لهذا المحتوى.

وعند النظر في هذه الأسئلة معًا، فإن السؤالين الأخيرين يحفزان على التركيز على الطبيعة غير الثابتة لمعنى المحتوى البصري، والإمكانات الكبيرة لتغير المعنى عبر إعادة الاستخدام والطريقة المتبعة في ذلك. وهذا لا يقتصر على ملاحظة المعنى الجديد الطارئ على هذا المحتوى في سياقه الجديد، وكيف أن ذلك يحوّر الهدف الذي وضعت له أصلًا، بل تتبع الآثار الناجمة عن إساءة توظيف المحتوى.

وهكذا فإن هذه المنهجية ليست معنية بمسألة التحقق وحسب، ولكنها أكثر اهتمامًا بتحليل معاني الصور وفق عمليات تستند إلى منهجيات من

تخصصــات متعــددة؛ مثــل تاريــخ الفنــون (Art History) ونظريــة الصــورة (Photo Theory).

أثنــاء عمليــات التطويــر لهــذا الإطــار والمحــاولات الأولــى لتطبيقــه مــع الصحفييــن، كنــا كثيـرًا مــا نسـمع منهـم بأنهـم لـم يكونـوا يعرفـون مـن قبـلُ عـن الصـور بهـذا القـدْر مـن التفاصيـل. وقـد أفـاد العديـد منهـم بـأن الإطـار سـاعدهم علـى اسـتيضاح مقـدار التعقيـد فـي الصـور عنـد توظيفها فـي عمليات التواصـل، وكانـوا علـى قناعـة بأنـه لا بـد مـن توفـر منهجيـة واضحـة للتعامـل معها ومع المعاني التي تتضمنها في السياقات المختلفة.

لـن تكـون هنالـك حاجـة فـي معظـم الحـالات للإجابـة عـن الأسـئلة العشـرين جميعهـا للوصـول إلـى فهـم شـامل وكامـل لكافـة الجوانـب المتعلقـة بصـورة ما. فهـذه الأسـئلة موجـودة للعـودة إليهـا والاسـتئناس بهـا، ونحـن نجدهـا فـي غايـة الفائـدة أثنـاء التعامـل مـع صـور ومقاطـع فيديـو معقـدة وذات حساسـية عاليـة وتلاقـي رواجًـا كبيـرًا واهتمامًـا مـن وسـائل الإعـلام. وللتعـرف علـى الجانـب العملـي المتعلـق بهـذا الإطـار وأسـئلته العشـرين، سـنعرض الآن ثلاث دراسـات حالة تتعلق بأمثلة مهمّة من المملكة المتحدة والولايات المتحدة.

دراسة الحالة 1: نقطة الانهيار - يونيو 2016



ما هي الصورة؟

صورة "نقطة الانهيار" (Breaking Point) هي ملصق دعائي استخدمه حزب استقلال المملكة المتحدة (UK Independence Party)، ضمن حملته خلال استفتاء الاتحاد الأوروبي عام 2016، وفيه صورة التقطها المصور الصحفي جيف ميتشيل في أكتوبر 2015، لتسليط الضوء على أزمة اللاجئين.

ماذا يظهر في الصورة؟

صف طويل من اللاجئين السوريين والأفغان يسيرون تحت مراقبة الشرطة في سلوفينيا من الحدود بين كرواتيا وسلوفينيا وصولًا إلى مخيم بريزيسي (Brezice) للاجئين.

الملصقُ الدعائي (البوستر) استخدم نسخة مقتطعة من الصورة وأضاف عليها عبارة "Breaking Point: The EU has failed us all" (نقطة الانهيار: الاتحاد الأوروبي خذلَنا جميعًا)، وفي الشريط السفلي كتب عليها "We must break free of the EU and take back

"control of our borders (علينا أن نتحرر من الاتحاد الأوروبي ونستعيد السيطرة على حدودنا). ولأن المهاجرين في الصورة يبدون وكأنهم مندفعون نحو الأمام بشكل جماعي لا سبيل لوقفه، كان لها أثر بصري على المشاهد.

من أنشأ المحتوى؟

شركة دعاية وإعلان بريطانية مقرها إدنبرة واسمها "Family Adver-tising Ltd"، وقد وقع اختيار حزب استقلال المملكة المتحدة لحملتها للترويج لخيار الانفصال عن الاتحاد الأوروبي.

ما معنى المحتوى؟

لم يقم الحزب المعنيّ بالحملة إلى إساءة تمثيل المحتوى، ولكنه أضفى عليه معنى إضافيًا عبر النصوص التي استخدمها. وباللعب على العاطفة السائدة لدى البعض من معاداة المهاجرين والعنصرية، ركّز هذا التلاعب على توليد المزيد من الرهاب ضد اللاجئين والمهاجرين، بناء على ادعاءات زائفة واتهامات غير دقيقة بشأن سياسات الحدود في الاتحاد الأوروبي.

ما الذي يعنيه المحتوى؟

في نوفمبر 2019، وفي الفترة السابقة للانتخابات العامة في المملكة المتحدة، استخدمت الحملة المؤيدة للانفصال عن الاتحاد الأوروبي نسخة مقصوصة من هذه الصورة نفسها ونشرتها ضمن حملة مناهضة للهجرة على تويتر، وهو استخدام يرتبط بشكل واضح بالملصق الإعلامي الذي استخدمه حزب استقلال المملكة المتحدة عام 2016.

ما الأسئلة الأخرى التي يمكن طرحها؟

هل تم نشر الصورة من جهة رسمية أو غير رسمية؟

الطرف الأساسي المسؤول عن إنشاء الصور ونشرها هو حزب استقلال المملكة المتحدة، وهو حزب سياسي رسميّ، وليس من قبيل الأطراف التي يتوقع عادة أن تكون منخرطة في نشر المعلومات الزائفة أو المضللة.

هل الصور مشابهة أو مرتبطة بصور أخرى؟

البعض وجد ارتباطًا بين الصورة وبين البروباغندا النازية، وهي مشابهة لصور أخرى سابقة ذات رسالة معادية للمهاجرين، وتاريخ طويل في الملصقات السياسية في المملكة المتحدة التي تستخدم صور "الطوابير"، مثل هذه الصورة التي استخدمها حزب استقلال المملكة المتحدة في مايو 2016 والتي تركز على مسألة الهجرة القادمة من الاتحاد الأوروبي.

نتائج ثلاث يمكن استخلاصها:

- الأحزاب السياسية الرسمية والسياسيون قد يشاركون في نشر المعلومات الزائفة.
- المعلومات الزائفة لا تتضمن بالضرورة استخدام صور مفبركة أو إساءة تمثيل للمحتوى المتضمن فيها، فالصور قد تُستخدم أحيانًا لدعم رسالة تسيء تمثيل موقف عام.
- بعض أنواع المعلومات الزائفة يتطلب مقاربة تتجاوز مسألة التحقق. فثمة حاجة للتحري بشكل نقدي لمعرفة كيفية توظيف الصور والتلاعب بها، وتحديد المعنى والأثر المترتب على ذلك.

أمثلة على التغطية الإعلامية لهذه الحالة:

الغارديان:

Nigel Farage's anti-migrant poster reported to police

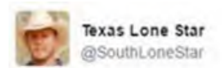
الجزيرة الإنجليزية:

Brexit: UKIP's 'unethical' anti-immigration poster

الإندبندنت:

Nigel Farage accused of deploying Nazi-style propaganda as Remain crash poster unveiling with rival vans

دراسة الحالة 2: صورة جسر "ويستمينستر"، مارس 2017




ما هي الصورة؟

تغريدة من حساب يظهر أن صاحبه رجل أبيض من تكساس، حازت تغريدته على قدر كبير من التفاعل. تبين لاحقًا أن الحساب يدار من قبل وكالة أبحاث الإنترنت الروسية (Internet Research Agency)، واستخدمت لأغراض نشر المعلومات الزائفة والمضللة. نشرت التغريدة صورة بعد الهجوم الإرهابي الذي وقع على جسر ويستمينستر في لندن في 22 مارس 2017.

ماذا تظهر الصورة؟

امرأة مسلمة تتجاوز مجموعة من الأشخاص على يمينها مجتمعين حول

شخص على الأرض بعد أن تعرض لإصابة بالهجوم الإرهابي. أما النص الذي استخدم مع الصورة فهو جزء من خطاب رهاب الإسلام، يدعي أن المرأة العابرة تتجاهل بشكل مقصود معاناة الشخص المصاب على الأرض، إضافة إلى استخدام وسم (هاشتاغ) معاد للإسلام أيضًا.

من أنشأ المحتوى؟
موظف في وكالة أبحاث الإنترنت الروسية يدير حسابًا على تويتر باسم المستخدم SouthLoneStar@، ولكن لم يكن ذلك معروفًا في وقت نشر التغريدة. أما الصورة الأصلية نفسها فقد التقطها المصور الصحفي جيمي لوريمان.

ما الذي عناه المحتوى المنشور؟
في مارس 2017، بدت التغريدة وكأنها قد نشرت من رجل أبيض يمينيّ من تكساس، فسّر الصورة على أنها لامرأة مسلمة لم تكترث بما حصل للشخص المصاب جرّاء الهجوم، ملمّحًا إلى أن هذا هو ديدن كل المسلمين.

ماذا يعني المحتوى الآن؟
تعتبر هذه التغريدة دليلًا على أن وكالة أبحاث الإنترنت الروسية تنشر بشكل متعمَّد معلومات مضلّلة ضدّ المسلمين في أعقاب هجوم إرهابي.

ما الأسئلة الأخرى التي يمكن طرحها؟
ما هي ردود الأفعال التي حصدتها الصورة؟
لقيت التغريدة صدى واسعًا في وسائل الإعلام السائدة، ونشرَتها العديدة من الصحف في المملكة المتحدة، وتكرر نشرها في بعض الأحيان. وبالرغم من إدانة العديد من هذه المقالات لصاحب الحساب (-South@ LoneStar)، فإنها عملت على نقل التغريدة من وسائل التواصل الاجتماعي إلى عموم الناس. وبعد هذا الانتشار والزخم اضطرت المرأة التي ظهرت في الصورة للخروج والتعليق، وقالت إنها كانت في حالة صدمة شديدة بعد الهجوم، وقالت: "لقد تعرضت لصدمة هائلة عندما

شهدت الهجوم الإرهابي الصادم والمرعب، لكن ذلك لم يكن نهاية الأمر، فقد كان عليّ فوق ذلك أن أجد صورتي منتشرة على وسائل التواصل الاجتماعي وأواجه اتهامات من أشخاص لم يروا سوى اللباس الذي أرتديه، وتوصلوا إلى استنتاجات مبنية على الكراهية ورهاب الأجانب".

هل الصورة مشابهة أو مرتبطة بصور أخرى؟

الصورة التي انتشرت على نطاق واسع كانت واحدة من بين سبع صور أخرى التقطت للفتاة، بعضها أظهر بوضوح أنها كانت في حالة صدمة، ولم تنتشر هذه الصور إلا في عدد قليل من وسائل الإعلام.

كم بلغ مدى انتشارها وكم امتدّت مُدّةُ رواجها؟

تفاعُل وسائل الإعلام السائدة مع الصورة زاد من انتشارها، لكن لم يستمر ذلك سوى عدّة أيام، وتراجع الاهتمام بالصورة بعد ذلك بشكل كبير. أعيد نشر الصورة مجددًا في نوفمبر 2017، حين تمّ اكتشاف أن الحساب الذي نشر التغريدة أول مرة يدار من قبل وكالة أبحاث الإنترنت الروسية، مع أنّ رواج هذه القصة كان أقل بكثير في وسائل الإعلام السائدة مقارنة بالزخم الذي حازته القصّة الأصلية في مارس.

نتائج ثلاث يمكن استخلاصها:

- لا يشترط في المحتوى البصري المضلل أن يكون مفبركًا بالكامل، بل يمكن أن يشتمل على عناصر فيها شيء من الحقيقة. الصورة التي تعاملنا معها حقيقية، ولكن تم التلاعب بالسياق وتشويهه، بالاعتماد على أن القارئ/المشاهد لا يعرف بالحقيقة ما كانت تشعر به الفتاة في تلك اللحظة.
- على الصحفي أن يفكر بشكل دقيق قبل أن يلفت المزيد من الانتباه إلى مثل هذه المعلومات المضللة التي تلعب على العواطف وتثير الجدل، بل قد تلحق الضرر أيضًا بطرف ما، حتى لو كان القصد إيجابيًا بهدف بيان الحقيقة وراءها.

- يجب الاهتمام بشكل أكبر بتصحيح الأخبار التي تعتمد على المعلومات المضللة والحرص على تصدير القصة الحقيقية والتركيز على نقلها للعامة. التغطية الضعيفة في نوفمبر بعد اكتشاف التلاعب الحاصل يعني أن العديد من القراء لم يعرفوا ربما أن التغريدة كانت ضمن حملة معلومات مضللة تقف وراءها جهة روسية.

أمثلة على التغطية الإعلامية لهذه الحالة:

People are making alarming assumptions about this photo of ‘woman in headscarf walking by dying man’ - Mirror

Who is the real monster?’ Internet turns on trolls who’ criticised ‘indifferent’ Muslim woman seen walking through terror attack - Daily Mail

British MP calls on Twitter to release Russian ‘troll factory’ tweets – The Guardian

دراسة الحالة 3: مواجهة عند نصب لينكولن التذكاري، يناير 2019



ما هو المحتوى؟

مقطع فيديو تظهر فيه مجموعة طلبة من ثانوية كوفينغتون الكاثوليكية (Covington Catholic High School)، يشاركون في مسيرة مناهضة للإجهاض، ويظهر فيها أيضًا رجل من السكّان الأصليين يدعى ناثان فيليبس، كان برفقة مجموعة من المواطنين الأمريكيين الآخرين من السكّان الأصلين في مسيرة خاصّة بهم.

ماذا يظهر في المحتوى؟

أحد الطلبة من الثانوية المذكورة يتواجه مع ناثان فيليبس، بعد أن التقت المظاهرتان في مكان يدعى "البلازا"، وكانت مجموعة كبيرة من الطلبة يرتدون قبعات حمراء كُتب عليها "Make America Great Again" (فلنُعِد العظمة إلى أميركا من جديد)، وبدا أنهم يتقدمون باتجاه فيليبس ويعترضونه. بدا المقطع وكأن فيليبس، وهو أحد السكان الأصليين، يواجه وحده مجموعة من الفتيان المتنمّرين ذوي التوجهات اليمينية المتطرفة.

من أنشأ المحتوى؟

ظهر الفيديو أولًا على منصة إنستغرام، ورفعه أحد المشاركين في المسيرة التي نظمها السكان الأصليون، وحاز المقطع على قرابة 200 ألف مشاهدة. بعد بضع ساعات وصل المقطع إلى تويتر، ليحصد 2.5 مليون مشاهدة، قبل أن يقوم صاحب الحساب الأصلي بحذفه. ثم أعيد نشر الفيديو عبر منصات التواصل الاجتماعي المختلفة، قبل أن يصل أخيرًا إلى وسائل الإعلام السائدة، وفي غضون 24 ساعة ظهرت عدة مقالات حول هذا الفيديو.

ما الذي عناه الفيديو؟

الرواية الأولى التي انتشرت عبر الإنترنت تعرض الفيديو باعتبار أنه مواجهة مباشرة بين فيليبس والطلبة الذين بدا أنهم يتعمدون السخرية من فيليبس والتجمع حوله.

ما الذي يعنيه الفيديو الآن؟

مقطع الفيديو الأطول عن الحادثة والذي ظهر بعد عدة أيام من انتشار الفيديو الأول يعكس صورة أكثر تعقيدًا. لقد كان في المشهد أيضًا مجموعة من "العبرانيين السود" والذين كانوا هم أيضًا يسخرون من المارّة، سواء من طلبة الثانوية أو السكان الأصليين. لقد كان الموقف متوترًا بين المجموعات الثلاثة، وكان فيليبس يحاول تهدئة الموجودين وإنهاء المشكلة، ومن تلك اللحظة بدأ تصوير الفيديو القصير الذي لاقى رواجًا كبيرًا.

ما الأسئلة الأخرى التي يمكن طرحها؟

ما هي المعلومات التي يجب معرفتها عن السياق؟

من دون توفر الفيديو الأطول وملاحظة وجود مجموعة أخرى من "العبرانيين السود" يؤججون التوتر القائم؛ لَما كان من الممكن معرفة السياق الكامل.

وبالرغم من العبارات العنصرية التي صدرت عن الطلبة في الفيديو، إلّا

أن مـا أدى إلـى ذلـك كان معقَّدًا، ولا يعنـي بالضـرورة أنهـم مجموعـة مـن المراهقين اليمينيين الذين تجمّعوا على رجل من السكان الأصليين.

على أي منصة تواصل اجتماعي انتشر الفيديو؟

ظهـر الفيديـو بدايـة فـي إنسـتغرام علـى حسـاب أحـد المشـاركين فـي المسـيرة الخاصـة بالسـكان الأصلييـن، ولكنـه لـم ينـل قـدرًا كبيـرًا مـن الاهتمـام. ثـم أعيـد تحميـل المقطـع علـى تويتـر ويوتيـوب مـن طـرف مسـتخدمين آخريـن، الأمـر الـذي ضاعـف رواج الفيديـو، لينـال فـي النهايـة اهتمامًـا مـن قبـل وسـائل الإعـلام السـائدة. وهكـذا فـإن الزخـم الـذي تولّـد حـول الفيديـو كان نتيجـة عمليـات إعـادة التحميـل علـى منصـات أخـرى، وليس بسـبب الفيديـو الأصلي الذي نشر على إنستغرام.

نتائج ثلاث يمكن استخلاصها:

- عنـد الانتشـار السـريع لمثـل هـذا المحتـوى البصـري المثيـر للتعاطـف علـى وسـائل التواصـل الاجتماعـي عـادة مـا يتـم إهمـال السـياق الأصلـي، وهـذا يعنـي تصديـر روايـة سـطحية انفعاليـة قـد تكـون منفصلة عن الحقيقة.
- جـادل بعـض الصحفييـن بـأن المقـالات ذات العلاقـة بالموضـوع زادت مـن حـدّة الجـدل وزادت مـن انتشـار روايـة غيـر مكتملـة عمّـا حصـل. وهـذا يعنـي أنـه فـي حـال غيـاب عمليـات التحقـق الملائمـة، فـإن وسـائل الإعـلام السـائدة قـد تسـاهم بـدون قصد فـي نشـر المعلومات الزائفة.
- السـرعة التـي انتشـر بهـا الفيديـو عبـر الإنترنـت تشـير إلـى أن العديـد مـن وسـائل الإعـلام السـائدة "خُدعـت" بالروايـة التـي تـم تداولهـا علـى وسـائل التواصـل الاجتماعـي، وأنهـا لـم تقـم بالتحقـق بالشـكل الكافـي. وقـد اضطـرت العديـد مـن المواقـع الإخباريـة إلـى التراجـع وتصحيـح المقـالات التـي نشـرتها بعـد أن ظهـرت المزيـد مـن التفاصيـل عـن الفيديو وسياقه، كما تعرض بعضها للملاحقة القضائية.

أمثلة على التغطية الإعلامية المتعلقة بهذه الحالة:

Native American Vietnam Vet Mocked And Surrounded By MAGA Hat-Wearing Teens - UNILAD

Outcry after Kentucky students in Maga hats mock Native American veteran - The Guardian

Fuller video casts new light on Covington Catholic students' encounter with Native American elder - USA Today

خلاصة

يمثل المحتوى البصري جزءًا كبيرًا مما يتم تداوله على وسائل التواصل الاجتماعي، وعلى الصحفيين أن يمتلكوا القدرة على طرح الأسئلة النقدية اللازمة وتقييم الصور من أجل تحديد ما تتضمنه ومعرفة المقصود منه. ولا شكّ أن هذا الانتشار السريع للمعلومات الزائفة في المحتوى المرئي يزيد من أهمية أن يتأنى الصحفيون عند التعامل مع القصص المرتبطة بهذا المحتوى والتحقق منها بشكل كامل قبل نشرها. الإطار الذي يتألف من 20 سؤالًا للتحقق من الصور على وسائل التواصل الاجتماعي هو أداة إضافية يمكن الاستفادة منها عند التحقق من الصور، ولاسيما حين تكون القصة قائمة على صورة أو مقطع فيديو أو شكل آخر من أشكال المحتوى المرئي الذي أشرنا إليها. لن يحتاج الصحفي إلى طرح الأسئلة العشرين جميعها للتحقق من كل صورة، ولكن الأسئلة الخمسة الأساسية تعدّ نقطة انطلاق جيدة في حال توفر المهارات الأساسية للتحقق، وذلك من أجل تطوير القدرة على كتابة قصص صحفية أكثر عمقًا ودقّة.

ملحق

فيما يلي القائمة الكاملة بالأسئلة العشرين التي يتألف منها الإطار المقترح، منها 14 سؤالًا سابرًا (Prompt Questions) وُضعت خصيصًا للتعامل مع المعلومات الزائفة أو المضللة. وقد أشرنا في هذا الفصل إلى أن ثمة أسئلة خمسة يُفضّل البدء بها. أما الأسئلة السابرة فتتعلق بالأطراف الفاعلة، أو الرسالة التي يتضمنها المحتوى، أو الطرف الذي يقوم بتفسير المحتوى المغلوط فيه أو المضلل:

- الطرف الفاعل: مَن الطرف الذي أنشأ المحتوى؟ ونشَره؟ وما هو دافعه؟
- الرسالة: ما هو شكل الصورة؟ وما سماتها؟
- المفسر: كيف تم تفسير الرسالة؟ وما ردّ الفعل الذي ترتّب على ذلك؟

1. ما هي الصورة؟

2. من صاحبها؟

3. ما الهدف الأصلي الذي وُضعت من أجله؟

أ. ماليّ، سياسي، اجتماعي، نفسي، أسباب أخرى؟

ب. من أو ما المقصود بالرسالة التي تمثلها الصورة؟

4. من الجمهور الذي تستهدفه الصورة؟

5. ما الذي يظهر في الصورة؟

6. ما المعنى الذي تفيده الصورة؟

أ. هل يسعى المحتوى إلى خداع الجمهور بادعاء أن الصورة من مصدر رسمي؟

ب. ما مدى دقة الرسالة التي تنقلها الصور؟

7. ما المعنى الذي أفادته الصورة بالأصل؟

أ. هل هنالك قصد لإلحاق الأذى أو التسبب بالتضليل؟

8. ما النص الذي ظهر على الصورة ليمنحها معنى محددًا؟

أ. هل النص دقيق أو مضلل أو يشتمل على معلومات مفبركة أو يهدف إلى التلاعب بالجمهور؟

9. ما المعلومات السياقية التي يجب معرفتها بشأن الصورة؟

أ. ما هي الرسالة التي تتضمنها الصورة قانونية؟

10. هل هي مشابهة أو مرتبطة بصورة أخرى؟

11. من أنتج الصورة؟

أ. هل هو طرف رسمي أو غير رسمي؟

ب. هل هي جهة منظّمة: وما مستوى التنظيم؟ (ليست جهة منظّمة، تنظيم بسيط، تنظيم معقد، تنظيم ضمن شبكة)

12. هل تم نشر الصورة على منصات التواصل الاجتماعي عبر الشخص الذي أنتجها؟

أ. هل نشرها إنسان، أم سايبورغ، أم حساب آلي؟

ب. هل هنالك قصد لإلحاق الأذى أو التسبب بالتضليل؟

13. إن لم يكن قد نشرَها الشخص الذي أنتجها، فمن نشرها على منصات التواصل الاجتماعي؟

14. هل أُنتجت الصورة خصيصًا للنشر على منصات التواصل الاجتماعي؟

15. إن لم تكن أنتجت للنشر على منصات التواصل الاجتماعي، فأين ظهرت بالأصل؟

16. على أي منصات التواصل الاجتماعي نشرت الصورة؟

أ. هل ولّدت الصورة ردود فعل أو تفسيرات مختلفة بين الناس؟ إن كان الأمر كذلك، فكيف؟

17. ما مدى رواج الصورة وكم ظلت رائجة؟

أ. فترة طويلة، فترة قصيرة، مرتبطة بحدث معين

18. كيف تفاعل الناس مع الصورة؟

أ. كيف تم التعاطي مع الصورة؟ هل تم إعادة إنتاج الرسالة التي تضمنتها الصورة؟

19. من هي الأطراف الأخرى التي استخدمتها على منصات التواصل الاجتماعي؟

20. هل لمشاركة الصورة على منصات التواصل الاجتماعي أي اعتبارات أخلاقية؟

استفدنا أثناء إعداد وتطوير هذا الإطار من المراجع التالية:

1. الشكل البياني بعنوان "Interrogating the work of Art" (الشكل 2.4 صفحة 39)، من كتاب "History of Art: A Student's Handbook"، الطبعة الخامسة، 2014، والصادر عن روتلدج.

2. كتاب "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making"، تحديدًا في الشكل البياني رقم 7، صفحة 28، بعنوان "Questions to ask about each element of an example of information disorder".

الفصل السادس: التعامل مع "الزَّيف العميق" وتقنيات التضليل الجديدة

سام غريغوري

سام غريغوري هو مدير البرامج في مؤسسة WITNESS (www.witness.org)، وهي مؤسسة تقدم خدماتها لمساعدة الناس على استخدام مقاطع الفيديو والتكنولوجيا لأغراض تتعلق بالدفاع عن حقوق الإنسان. له العديد من الإنجازات في مجال التكنولوجيا والمناصرة، ونال العديد من الجوائز، وهو خبير في الأشكال الجديدة من المعلومات الزائفة والمضللة المعتمدة على تقنيات الذكاء الاصطناعي، وله جهود رائدة في بيان ما تمثله هذه التقنيات الناشئة من فرص وتحديات على العمل الحقوقي والصحفي. سام رئيسٌ مشارك في مبادرة مجموعة خبراء الذكاء الاصطناعي وعلاقته بالإعلام.

في صيف عام 2018، نشر البروفيسور سيوي لاي (Siwei Lyi)، وهو باحث رائد في مجال الزيف العميق في جامعة ألباني (Albany)، ورقة بحثية تثبت أن الوجوه التي تَظهر في مقاطع الفيديو عميقة التزييف لا ترمش بنفس المعدل الذي يرمش به البشر الحقيقيون.

وسرعان ما تلقفتْ هذه الملاحظةَ العديدُ من المجلات والمواقع، مثل "فاست كومباني"، و"نيو سايئتست"، و"جيزمودو"، و"سي بي أس نيوز"، وغيرُها، ما ولّد قناعة لدى كثيرين بأنه قد باتت لدينا الآن طريقة موثوق بها للتعرف على مقاطع فيديو عميقة التزييف.

ولم تكد تمضي عدة أسابيع على نشر هذا البحث حتى وصل إلى هذا

الباحث عدد من مقاطع الفيديو عميقة التزييف تستخدم وجوهًا ترمش بشكل مماثل للطريقة التي يرمش بها البشر الحقيقيون. وهكذا فإن هذه الملاحظة لم تعد مفيدة ولا دقيقة، رغم أنّها كانت خللًا أساسيًّا في خوارزميات الزيف العميق في تلك الآونة، وبيانات التغذية التي كانت تستخدم في إنشائها. ولكنْ في غضون بضعة أشهر اختفت هذه المشكلة بعد التوصّل إلى حلّ لها.

يوضح هذا المثال حقيقة أساسية بخصوص التحري عن الزيف العميق وكشفه، وهي أن المقاربات التقنية تحقق الفائدة المتوقعة منها إلى أن تتمكّن التقنيات الخاصة بتطوير عمليات التزييف العميقة من التكيف وتجاوُز الخلل الذي يمكّن من الكشف عنها، وهكذا فإنه لا يمكن تخيّل وجود نظام مثاليّ أوحد للكشف عن عمليات التزييف العميقة.

لكن كيف سيتمكن الصحفيون إذن من التحقق من الزيف العميق وغيره من أشكال المحتوى المركّب؟

الخطوة الأولى تتمثل في فهم الطبيعة المراوغة لهذا العمل، والتنبه باستمرار للتطور التقني المستمر في هذا المجال. أما الأمر الثاني، فعلى الصحفي أن يتعلم ويطبق تقنيات التحقق الأساسية ويكون قادرًا على استخدام مختلف الأدوات المتوفرة للتحقق من محتوى ما واكتشاف ما إذا كان قد خضع للتلاعب، أو أنّه نتيجة عملية تزييف صناعية بالكامل. ويمكن الاطلاع على أساليب التحقق من الصور ومقاطع الفيديو التي تضمنها دليل التحقق الأول، إضافة إلى المصادر الخاصة بالتحقق من المواد البصرية والمتوفرة في دليل مؤسسة "فيرست درافت". ويجب على الصحفيين أخيرًا أن يدركوا أننا في بيئة يشيع فيها وبشكل متزايد ادعاء أن محتوى ما هو زيف عميق، وهذا يعني أن القدرة على التحقق من صحة صورة أو مقطع فيديو ما؛ لا يقل أهمية عن اكتشاف حدوث تلاعب فيها.

يحاول هذا الفصل البناء على هذه المبادئ الأساسية للتحقق من عمليات

التزييف العميقة، ولكن من المهم في البداية أن نتفق معًا على فهم أساسي للتزييفات العميقة (DeepFakes)، والمحتوى الإعلامي المركّب (Synthetic Media).

ما هو الزيف العميق والمحتوى الإعلامي المركّب؟

التزييفات العميقة هي أشكال جديدة من التلاعب الصوتي البصري تتيح إمكانية توليد محاكاة واقعية لوجه شخص ما أو صوته أو حركاته، بحيث يبدو كأن هذا الشخص قد قال أو فعل أمرًا، وهو لم يقم به على الحقيقة.

وقد ازدادت سهولة توليد مثل هذا الشكل من المحتوى، والذي بات لا يتطلب سوى قدر بسيط من التغذية (Source Images) لبناء المحتوى عميق التزييف. هذه العمليات من التزييف تؤثر بشكل كبير حاليًا على النساء بشكل خاص، وذلك لأن العديد يستخدمونها في إنشاء صور ومقاطع فيديو جنسية باستخدام وجه المرأة وصوتها، وهنالك خشية مستمرة من أن يتزايد تأثير عمليات التزييف العميقة في المجتمع ووسائل الإعلام وعمليات التحقق.

وتعد ظاهرة الزيف العميق واحدة من بين العديد من التطورات التي شهدها مجال الذكاء الاصطناعي في توليد المحتوى الإعلامي المركب. فهذه المجموعة من الأدوات والأساليب تتيح الفرصة لخلق تمظهُرات واقعية غير حقيقية لأشخاص يقولون أو يفعلون أشياء لم يفعلوها، إضافة إلى خلق صور لأشخاص أو أشياء وهمية، أو حتى لأحداث لم تقع حقيقةً.

وتساعد تقنيات المحتوى المركب حاليًا على الأشكال التالية من التلاعب والتزييف:

- إضافة أو إزالة بعض العناصر في مقطع فيديو.

- تعديل الخلفية في مقطع فيديو، كتغيير الحالة الجوية، بحيث يبدو المقطع الذي صُور في الصيف كأنه حصل في الشتاء.
- المحاكاة والتحكم في الفيديو بحركة الشفاه وتعابير الوجه أو حركة الجسد لشخص يظهر في المقطع. فبالرغم من أن النقاشات حول التزييفات العميقة تركز عادة على الوجوه، إلا أن ثمة تقنيات مختلفة تُعنى بالتحكم بحركة الجسم بأكمله، أو أجزاء محددة من الوجه.
- توليد محاكاة واقعية لصوت شخص محدد.
- إجراء تعديل على صوتٍ ما باستخدام "طبقة صوتية" لجندر مختلف، أو لشخص آخر.
- توليد صورة واقعية لشخص وهمي لا وجود له في الحقيقة، وهي تقنية تستخدم في مجالات أقل إشكالية، لتوليد صور لأطعمة أو حيوانات معينة.
- نقل وجه حقيقي من شخص إلى آخر، وهو ما يعرف عادة بالزيف العميق.

تعتمد هذه التقنيات بشكل أساسي ضمن عناصر أخرى على شكل من الذكاء الاصطناعي المعروف باسم "التعلم العميق" وما يعرف أيضًا باسم "الشبكات الخصومية التوليدية" (Generative Adversarial Networks).

من أجل توليد محتوى إعلامي مركّب، فلا بدّ من البدء بتجميع الصور أو مقاطع الفيديو الأصلية للشخص أو الأمر الذي نريد التلاعب به. تقوم الشبكة الخصومية التوليدية (GAN)، بإنشاء المحتوى المزيف، سواء كان ذلك محاكاة في مقطع فيديو لشخص حقيقي، أو عملية تبديل للوجوه من شخص إلى آخر، عبر استخدام شبكتين.

فالشبكة الواحدة تعمل على توليد إعادات خلق واقعية للصور الأصلية،

أما الشبكة الثانية فتعمل على الكشف عن هذا التزييف. ويتم تغذية هذه البيانات الخاصة بكشف التزييف بشكل عكسي إلى الشبكة التي تعمل على توليدها، ما يتيح لها الفرصة لتطوير الأداء.

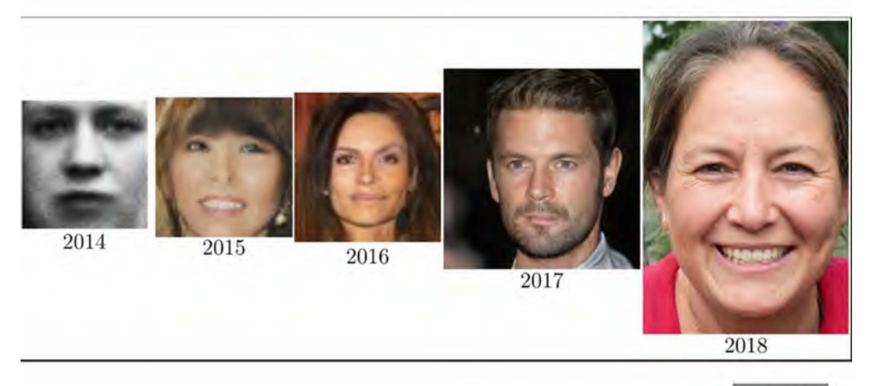
ومنذ نهاية العام 2019، حظيت العديد من هذه التقنيات -وخاصة تقنية توليد التزييفات العميقة- بقدر كبير من التطور الحاسوبي، بشكل ساعد على تحسين النماذج التي يتم العمل وفقها، إضافة إلى العمل بعد الإنتاج وفق بروتوكول "واجهة المعابر العامة" (CGI) من أجل تحسين النتيجة النهائية.

وبالرغم من بعض الشوائب التي ما تزال تعتري هذه العمليات، فإن البشر كثيرًا ما تعرّضوا للخداع وانطلت عليهم أشكال هذا المحتوى المزيف، فثمة أبحاث من مؤسسة "++FaceForesnsics" تشير إلى أن الناس لا يستطيعون الكشف عن الأنماط المستخدمة حاليًّا في تعديل حركات الشفاه، والتي تستخدم من أجل تعديل حركة شفاه شخص ما بشكل متّسق مع مقطع صوتي جديد مزيف، ما يعني أن البشر ليسوا قادرين بشكل طبيعي على الكشف عن التلاعب الحاصل عبر عمليات المحتوى الإعلامي المركب.

كما تَلزم الإشارة إلى أن عمليات التزييف الصوتي تتقدم بشكل أسرع من المتوقع؛ حتى إنها أصبحت متوفرة تجاريًا. فلنأخذ مثلًا واجهة برمجة التطبيقات السحابية من جوجل الخاصة بتحويل النص إلى كلام، والتي توفّر ذلك باستخدام صوت يحاكي الصوت البشري. كما تناولت بعض الأبحاث إمكانية تحويل نص ما إلى مقطع فيديو حواري يشتمل على الصوت والصورة معًا.

أضف إلى ذلك كله أن ما نلاحظه حاليًا من الاهتمام التقني والتجاري بهذه الجوانب يعني أن إنشاء المحتوى المركّب سيكون عملية أكثر سهولة وأقل تكلفة في المستقبل. الصورة أدناه تبين مثلًا مقدار السرعة

التي تطورت بها تكنولوجيا توليد الأوجه في الآونة الأخيرة:



وبالنظر إلى الطبيعة المراوغة لهذه الشبكات، فإنها تتحسن باستمرار مع مرور الوقت بالاعتماد على البيانات التي تحصل عليها من عمليات التزييف الناجحة إضافة إلى عمليات الكشف عن التزييف، وهذا يعني ضرورة التأكّد باستمرار من فعالية الطرق المستخدمة في الكشف عن التزييف والتطوير عليها.

نظرة على آخر التطورات في مجال الزيف العميق والمحتوى المركّب

لا يزال الزيف العميق والمحتوى الإعلامي (البصري الصوتي) المركّب غير واسع الانتشار، باستثناء استغلالها فيما يتعلق بالصور الجنسية بغير موافقة أصحابها. ويشير تقرير صادر عن مؤسسة "Deep Trace Lab" إلى أن انتشار هذه الأشكال من المحتوى حتى سبتمبر 2019 كان مقتصرًا في حوالي 95% منه على هذه الأغراض الجنسية، سواء ما تعلق منها بالشخصيات الشهيرة أو الممثلات الإباحيات أو حتى الأشخاص العاديين. كما أن بعض الناس قد بدؤوا بالشكّ حتى في أمثلة حقيقية من المحتوى؛ ظنًّا منهم بأنها مجرد حالات من التزييف العميق.

في ورش عمل من تنظيم مؤسسة "WITNESS"، قمنا بمراجعة أشكال التهديد المحتملة مع عدد من المشاركين من المجتمع المدني، كان من بينهم ممثلون لوسائل إعلامية شعبية، وصحفيون مهنيون، ومختصون في مجال التحقق وباحثون في مجال المعلومات الزائفة والمضللة، إضافة إلى مختصين في مجال "استخبارات المصادر المفتوحة" (OSINT). وقد تم العمل على تحديد النطاقات التي من الممكن أن يتسع فيها توظيف هذه الأشكال من المحتوى وزيادة مستويات التهديد التي تنطوي عليها، أو خلق تهديدات جديدة، أو التغيير من طبيعة تهديدات قائمة أو تعزيزها.

كما قام المشاركون بتحديد التحديات والمخاطر التي تواجه الصحفيين والعاملين في مجال التحقق والمحققين الذين يعتمدون على المصادر المفتوحة، والهجمات المحتملة على عملياتهم. وأشار بعض المشاركين أيضًا إلى الإشكال الذي يثيره استسهال وسم أي محتوى "مزيف" بأنه "زيف عميق" وما يثيره ذلك من خلط بين الأمرين.

وقد جرى التأكيد في مختلف هذه السياقات على أهمية مقاربة الزيف العميق في سياق المنهجيات المتبعة والمعروفة المتعلقة بالتحقق والتوثق من المحتوى. فالتزييفات العميقة والمحتوى الإعلامي المركّب تدخل ضمن حملات مؤامرة وتضليل قائمة، بالاعتماد على أساليب ومراوغات متطوّرة يتم اللجوء إليها في هذا المجال.

وفيما يلي بعض أهم التهديدات التي تم تسليط الضوء عليها:

- تشويه سمعة ومصداقية الصحفيين والناشطين الحقوقيين، وذلك بالبناء على ما هو قائم من أشكال من التحرش والعنف الرقميين، والتي تستهدف عادة النساء والأقليات. وثمة العديد من الأمثلة على هجمات اعتمدت على مقاطع فيديو معدّلة تستهدف صحفيات بالتحديد، مثلما حصل مع الصحفية الهندية البارزة رنا أيوب.
- استهداف شخصيات عامة عبر فبركة صور جنسية أو صور تشتمل على عنف جندري إضافة إلى استخدامات أخرى لما يعرف

بالأشباه الواقعيين. وقد يكون السياسيون المحليون هنا من أكثر الأطراف استهدافًا بهذا النوع من الفبركات، وذلك بسبب توفر العديد من الصور الخاصة بهم على الإنترنت، إضافة إلى وضعهم المؤسساتي الهشّ مقارنة بالسياسيين على المستوى الوطني والذين يمتلكون عادةً وسائل تأثير أعلى تساعدهم على التصدي لمثل هذه الهجمات. كما أنهم كثيرًا ما يشاركون كمصادر أولية في التغطيات الإخبارية التي تتجاوز المحلي إلى الوطني.

- تقليد العلامات التجارية المعروفة وتشويه سمعتها، وذلك عبر تقنيات التعديل داخل الفيديوهات أو غيرها من الطرق، بغرض توريط علامة تجارية لشركة أو منظمة أو مؤسسة إعلامية أو جهة حكومية في نوع من المحتوى المزيف.
- محاولة ضخّ محتوى ينتجه مستخدمون (UGC) غير حقيقيين في دورة الأخبار، بالإضافة إلى أساليب أخرى مثل "اختراق المصدر" (Source-Hacking)، أو مشاركة محتوى متلاعَب به مع صحفيين في سياق الأخبار العاجلة، وكل ذلك بهدف توريط الصحفيين في إشاعة هذا النوع من المحتوى.
- استغلال بعض نقاط الضعف في جمع الأخبار أو إعداد التقارير، مثل عمليات البث التي تعتمد على كاميرا واحدة (كما أشار فريق محتوى المستخدمين في رويترز)، وعمليات جمع المعلومات في ظروف استثنائية مثل مناطق الحرب أو الكوارث وغيرها.
- في ظل استمرار تفشي التزييفات العميقة وزيادة سهولة إنشائها بكميات كبيرة، فإنها قد تعني اضطرار تعامل المؤسسات والجهات المختصة بالتحقق والتثبت مع قدر هائل من المحتوى قد يتجاوز إمكاناتها ويؤدي إلى تشتت جهودها.
- سيتضاعف الضغط على المؤسسات العاملة في مجال جمع الأخبار والتحقق منها لإثبات حقيقة أمر ما، بالإضافة إلى إثبات أن محتوًى ما ليس مزيفاً. وقد تستغل السلطات أسلوب الإنكار المقبول؛ لإثارة الشكّ بشأن أي محتوى.

التحقق من التزييفات العميقة: خطوة أولى

بالنظر إلى طبيعة التحريات الإعلامية والتقنيات الناشئة في مجال الزيف العميق، فإن علينا أن نتفق على أن غياب الدليل الذي يفيد بأن ثمة محتوى قد تم التلاعب به لن يصلح لأن يكون دليلًا حاسمًا للقطع اليقيني بأن ذلك المحتوى لم يخضع فعلًا للتلاعب به.

فعلى الصحفيين والعاملين في مجال التحقق أن يطوروا ذهنية من الشكّ المعقول بشأن ما يتعاملون معه من صور ومقاطع فيديو أو مقاطع صوتية. ومن الضروري أن يكون لدينا افتراض بأن هذه الأشكال من المحتوى الإعلامي ستخضع للمزيد من الشكّ وعمليات التحرّي، وذلك بسبب تزايد المعرفة بشأن تفشي الزيف العميق والتخوف منه. ومن المطلوب أيضًا تطوير القدرة على التعامل بشكل عالي الكفاءة مع أدوات التحقق من المحتوى.

وبالبناء على هذه الذهنية والإمكانيات الأساسية في التحقق من المحتوى، لا بدّ أن تراعي أي منهجية لتحليل التزييفات العميقة والتلاعب بالمحتوى الإعلامي المركّب العمليات الآتية:

1. مراجعة المحتوى لتحديد ما إذا كان يشتمل على أية آثار لتعديلات أو تشويهات تدلّ على عمليات تركيب اصطناعية.

2. تطبيق المنهجيات المتوفرة الخاصة بالتحقق والتحري من مقاطع الفيديو.

3. الاستفادة من الأساليب الخاصة بالتحقق والتحري والتي تعتمد على تقنيات الذكاء الاصطناعي.

مراجعة المحتوى لتحديد ما إذا كان يشتمل على أية آثار قد تدل على حدوث تعديلات أو تشويهات تدلّ على عمليات تركيب اصطناعية

وتعد هذه الطريقة الأقل صرامة فيما يتعلق بالكشف عن الزيف العميق وغيره من أشكال التلاعب بالمحتوى المركّب، خاصة بالنظر إلى التطورات التقنية المستمرة في هذا المجال. ويمكن القول: إن هذه الطريقة قد تفيد عند التعامل مع التزييفات العميقة رديئة الجودة والتي قد تشتمل على أخطاء بيّنة، من قبيل:

- انحرافات محتملة عند جبهة الوجه أو طرفها من جهة منبت الشعر أو عند ملاحظة تجاوز الرأس لمدى معين من نطاق الحركة.
- ضعف التفاصيل المتعلقة بالأسنان.
- النقاء المفرط في البشرة.
- عدم رمش العينين.
- الثبات الملحوظ على المتحدث دون وجود أي حركة طبيعية بالرأس أو التعابير الأخرى.
- ملاحظة خلل في الصورة عند تحرك الشخصية وتغيير موقع الوجه بالنسبة للمشاهد.

بعض أوجه الخلل قد تكون حاليًا واضحة عند تحليل إطار بإطار للفيديو (Frame-by-Frame)، بحيث يتم استخلاص مجموعة من الإطارات لمراجعتها بشكل منفصل، وإن كان ذلك لن يفيد في تحديد الخلل الحاصل عند الانتقال من حركة أمامية إلى جانبية، فهذا النوع من الخلل يكون أكثر وضوحًا في التحليل التسلسلي (Sequence)، ما يعني ضرورة الاعتماد على كلتا الطريقتين.

تطبيق المنهجيات المتوفرة الخاصة بالتحقق والتحري من مقاطع الفيديو

مثلما هي الحال مع الأشكال الأخرى من التلاعب بالمحتوى والتزييفات الضحلة "ShallowFakes"، مثل التعديل البسيط على مقاطع الفيديو أو

نشرها في غير سياقها الأصلي، فإنه يلزم عند التعامل مع الزيف العميق الانطلاق من أرضية راسخة من الإلمام بممارسات التحقق وإتقانها. هذا بالإضافة إلى ممارسات التحقق المعمول بها في مجال "استخبارات المصادر المفتوحة". وتعد الفصول ودراسات الحالة الخاصة بالتحقق من الصور ومقاطع الفيديو في دليل التحقق الأول نقطة بداية جيدة.

وبما أن معظم التزييفات العميقة حاليًا ليست مختلقة بشكل كامل، بل تعتمد على إجراء تعديلات على مقاطع الفيديو، فإنه يمكن استخدام إطارات (Frames) الفيديو للبحث عن نسخ أخرى من المقطع عبر آلية البحث العكسي بالصور. كما يمكن النظر بشكل دقيق في المقطع لتحديد ما إذا كان المشهد والمعالم المتضمنة متوافقة مع صور الموقع نفسه عند التحري عنه في خدمة "عرض شوارع جوجل" (Google Street View).

يمكن كذلك الاستفادة من المنهجيات الخاصة بتحليل أنماط مشاركة المحتوى وانتشاره، عبر تحديد: مَن الطرف الذي نشر المحتوى؟ وأين نشره؟ وكيف نشره؟ إذ يساعد التحري عن هذه المعلومات على تشكيل انطباع أولي عن مدى مصداقية المحتوى سواء كان صورة أم مقطع فيديو.

فلا يمكن الاستغناء هنا عن الأساسيات المتعلقة بتحديد المصدر والتوقيت والتاريخ والدافع وراء محتوى ما، لمعرفة ما إذا كان المصدر والمحتوى الذي ينشره حقيقيًا. (لمراجعة هذه الأساسيات يمكن الاطلاع على الدليل الصادر عن فيرست درافت). ومن الضروري كذلك، كالعادة، محاولة التواصل مع الشخص أو الأشخاص الذين ظهروا في مقطع الفيديو للحصول على تعليق منهم لو أمكن، أو لطلب أي معلومات تؤكّد أو تنفي صحّة المقطع.

ثمة أدوات جديدة تعكف على تطويرها بعض الهيئات الحكومة والمؤسسات الأكاديمية والصحفية والمنصات والمختبرات المختصة، للمساعدة على كشف المحتوى المزيف وزيادة القدرة على الوصول إلى أدوات التحرّي عن المحتوى والتحقق منه. لكن يجدر بالصحفي أن يتعامل مع هذه

الأدوات كوسيلة للاستئناس بنتائجها ومقارنتها بالملاحظات التي جمعها عبر أفضل منهجيات التحقق المعروفة.

ومن الأدوات المجانية التي يمكن الاستفادة منها في هذا المجال:

- **FotoForensics**: وهي أداة للتحقيق في الصور، تساعد على تحليل مستوى الخطأ (Error Level Analysis)، وذلك للكشف عن أي عناصر تمت إضافتها إلى الصورة.
- **Forensically**: وهي حزمة من الأدوات التي تساعد في الكشف عن عمليات الاستنساخ، وتحليل مستوى الخطأ، والبيانات الوصفية للصورة (Metadata)، وعدد من العمليات الأخرى للتحقق من الصور.
- **InVID**: إضافة على متصفح الإنترنت (Extension) يساعد على تقطيع الفيديو إلى إطارات، وإجراء عملية بحث عكسي للتنقيب في عدة محركات بحث، وتحسين جودة الإطارات والصور عبر عدسات التكبير، وتطبيق فلاتر التحرّي على الصور الثابتة (Still Images).
- **Reveal Image Verification Assistant:** أداة تعتمد على نطاق واسع من الخوارزميات الخاصة بالكشف عن التلاعب بالصور والتعديل عليها، إضافة إلى خاصية تحليل البيانات الوصفية للصور، وتحديد الموقع، واستخلاص "ثمبنيل" بصيغة الملف الصوري المتبادل (EXIF)، وتمكين البحث العكسي عن الصور عبر جوجل.
- **Ghiro:** أداة تحليل رقمية عبر الإنترنت، تعتمد على المصادر المفتوحة.

جميع هذه الأدوات في القائمة السابقة مخصصة للتحقق من الصور، لا من مقاطع الفيديو، وهذه نقطة ضعف ما يزال العمل جاريًا على تجاوُزها في هذا المجال. لذلك لا يزال من الضروري عند التحقق من

مقاطع الفيديو استخلاص بعض الصور والعمل على تحليلها بشكل منفصل، وهذا ما يمكن أن تساعد فيه أداة InVID.

وتعتمد فعالية هذه الأدوات عند التعامل مع مقاطع فيديو عالية الدقة وغير مضغوطة جرى عليها بعض التعديلات عبر إضافة بعض العناصر داخلها أو إزالتها. وستتراجع الفائدة العملية من هذه الأدوات في حال كان مقطع الفيديو مضغوطًا، أو تكرّر تنزيله وحفظه ومشاركته على وسائل التواصل الاجتماعي أو منصات مشاركة مقاطع الفيديو.

إن كنت تبحث عن أدوات تحليل جديدة لأي محتوى إشكالي من الصور أو مقاطع الفيديو قد تشكّ بأنه تعرض لعملية تزييف عميقة، فإنه من الضروري متابعة الأدوات التي يعمل الأكاديميون على تطويرها ومشاركتها. وتضمّ جامعة نابولي أحد أبرز المراكز البحثية الرائدة في هذا المجال، والذي يقدم إمكانية الاستفادة عبر الإنترنت من أداة تساعد في الكشف عن بصمات الكاميرا (Noisrprint)، والكشف عن عمليات القص والتركيب في الصور (Splicebuster)، والكشف عن عمليات تحريك العناصر (Copy-Move) داخل نفس الصورة أو مقطع الفيديو.

ومع التطور الحاصل في عالم الزيف العميق وتركيب المحتوى، فإن ثمة أشكالًا جديدة من عمليات التحقق والتحليل اليدوية والآلية يتم تطويرها وتحسين أدائها ودمجها ضمن أدوات التحقق المعروفة التي يستخدمها الصحفيون والعاملون في مجال التحقق من المحتوى، إضافة إلى إمكانيات دمجها منهجيات قائمة على التعامل مع المنصات المختلفة. ومن الضروري أن يحرص الصحفي على الاطلاع باستمرار على أحدث الأدوات التي يجري تطويرها وتوفيرها من قِبل المؤسسات المختصة أو الناشطين في هذا المجال والاستفادة منها، وأن يكون في المقابل حذِرًا من الإفراط في الاعتماد عليها.

الأساليب الجديدة للتحقق بالاعتماد على الذكاء الاصطناعي

حتى مطلع العام 2020 لم يكن هنالك أي أداة تحقق تعتمد على الشبكات

الخصوصية التوليدية (GAN)، لكن من المتوقع توفر بعض هذه الأدوات قريبًا، سواء كانت ملحقة في برامج أخرى، أم أدوات مدمجة على المنصات.

وللاطلاع على آخر عملية مسح لأحدث الأدوات المتوفرة في مجال التحقق الإعلامي، يمكن الاطلاع على هذه الدراسة للباحثة لويزا فيردوليفا بعنوان "Media Forensics and DeepFakes: An Overview".

هذه الأدوات ستعتمد بشكل عام على بيانات تغذية (أمثلة) من وسائط مركّبة بالاعتماد على الشبكات الخصومية التوليدية (GAN)، والتي ستُستخدم من أجل الكشف عن حالات أخرى تَستخدم أساليب مماثلة أو مشابهة.

فعلى سبيل المثال، ثمة برامج مثل FaceForensics++ تعمل على توليد التزييفات بالاعتماد على بيانات خاصة بتزييفات عميقة سابقة، ثم تعمل على استخدام هذا الحجم الضخم من الصور الزائفة كبيانات تدريب للخوارزميات للكشف عن الزيف، وهذا يعني بطبيعة الحال أنها قد لا تكون فعالة للكشف عن أساليب وتقنيات التزييف الأحدث.

وستكون هذه الأدوات مناسبة للكشف عن الوسائط المولّدة بالشبكات الخصومية التوليدية بشكل أكبر مما توفره تقنيات التحرّي المتوفرة حاليًا. كما أنها ستعزز من جودة أداء الأدوات الجديدة للتحري عن الوسائط المفبركة ذات القدرة الأكبر على التعامل مع التطورات الحاصلة على صعيد التزييف العميق والتركيب. لكنها في المحصلة لن تكون مكفولة النتائج دومًا، وذلك كما أسلفنا يعود إلى الطبيعة المراوغة للتطويرات المستمرة التي تشهدها عمليات التزييف والتركيب، ما يعني بشكل أساسي أن أي محاولة للكشف عن التركيب والتزييف العميق يجب أن تتضمن أكثر من عملية تحقق واحدة تعتمد على أساليب مختلفة دون الاكتفاء بطريقة واحدة.

يشهد ميدان التزييفات العميقة والمحتوى المركب تطورات سريعة، كما أن التقنيات المستخدمة باتت متوفرة بشكل أوسع على المستوى التجاري وهذا يتضمن أنها باتت أيضًا أسهل استخدامًا، ولا تحتاج إلى قدر كبير من المحتوى الأصلي من أجل التوصّل إلى التزييف.

نشهد في المقابل بروز تقنيات جديدة للكشف عن هذا النوع من الفبركات، ويتم العمل على تضمينها في المنصّات الخاصة بالتحقق والأدوات التي يستخدمها الصحفيون والعاملون في مجال استخبارات المصادر المفتوحة، لكن المنهجية الأسلم في التحقق منها هي استخدام الأساليب المعروفة في التحقق من الصور ومقاطع الفيديو، إضافة إلى الأدوات الخاصة بفحص هذا المحتوى والتي تساعد على الكشف عن عمليات التلاعب بالصور. وغنيّ عن القول: إنه لا يمكن الاعتماد على استراتيجية تكتفي بما تراه العين المجرّدة للكشف عن الزيف العميق.

الفصل السابع: المراقبة والتحري داخل المجموعات المغلقة وتطبيقات المراسلة

كلير واردل

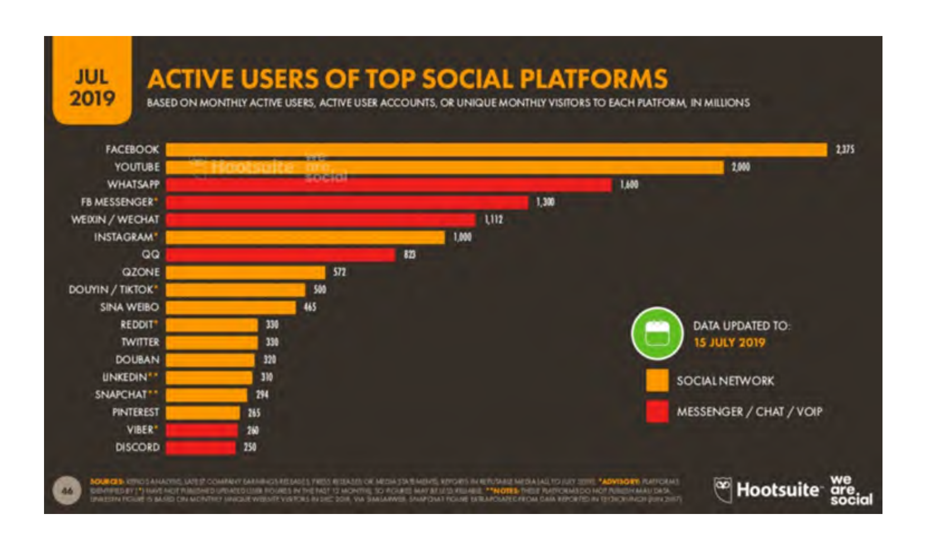
كلير واردل هي مديرة التوجيه الإستراتيجي والأبحاث في مؤسسة "فيرست درافت" (First Draft)، وهي مؤسَّسة عالمية غير ربحية لدعم الصحفيين والأكاديميين والتقنيين الذين يسعون إلى التعامل مع التحديات المتعلقة بمسائل الثقة والحقيقة في العصر الرقمي. حازت كلير واردل على زمالة مركز شورنستين للإعلام والسياسة والسياسات العامة في كلية كينيدي بجامعة هارفرد، وشغلت منصب مديرة الأبحاث في مركز تاو للصحافة الرقمية في كلية الدراسات العليا في الصحافة بجامعة كولمبيا، إضافة إلى مديرة شؤون وسائل التواصل الاجتماعي في المفوضية السامية للأمم المتحدة لشؤون اللاجئين.

في مارس 2019، تحدث مارك زوكربيرغ عن أهمية مسألة الخصوصية في فيسبوك، بمعنى أن المنصّة ستولي اهتمامًا أكبر بمجموعات فيسبوك، بعد أن لاحظت إقبال الناس المتزايد على التواصل مع مجموعات أصغر من الناس في مساحات ذات خصوصية أكبر. وقد لاحظ المهتمون بهذا المجال خلال السنوات الماضية تزايد هذه الأهمية للمجموعات الصغيرة على وسائل التواصل الاجتماعي.

في هذا الفصل سأتحدث عن المنصات والتطبيقات المختلفة والتحديات المتعلقة بمراقبتها، مع تعقيب في نهاية الفصل حول أخلاقيات هذا النشاط.

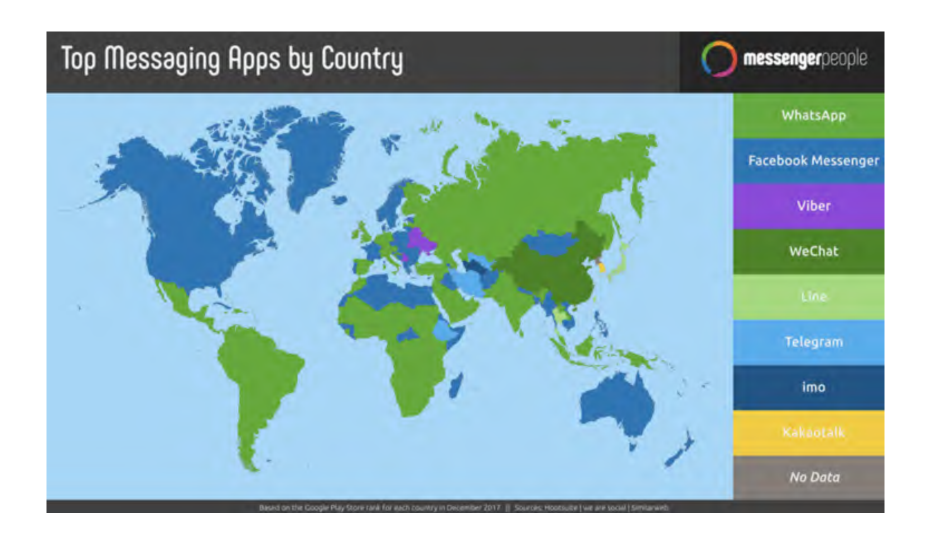
المنصات والتطبيقات المختلفة

تُظهر آخر الأبحاث الصادرة عن مؤسسة "We Are Social" استمرار هيمنة فيسبوك ويوتيوب، لكنها أظهرت أيضًا أن المنصات الثلاثة الأخرى الأكثر استخدامًا هي واتساب، وفيسبوك ماسنجر، وتطبيق وي تشات.



باتت تطبيقات المحادثة في العديد من المناطق حول العالم مصدرًا مهيمنًا للأخبار لدى الكثيرين، ولاسيما واتساب، وهذا هو الحاصل في دول عديدة مثل البرازيل والهند وإسبانيا.

ولا شك أن واتساب وفيسبوك ماسنجر يحظيان برواج كبير حول العالم، لكن ثمّة تطبيقات بديلة تهيمن في دول أخرى. ففي إيران يتصدّر تطبيق تليغرام، أما في اليابان فهنالك تطبيق "لاين"، وفي كوريا الجنوبية ستجد تطبيق "كاكاو توك"، بينما يهيمن تطبيق "وي تشات" في الصين.



ولكل واحد من هذه التطبيقات سمة عملية محدَّدة تتميز بها من سواها، سواء كان ذلك على صعيد التشفير والخصوصية أم إمكان إجراء المكالمات الجماعية، أم الخيارات المتعلقة بالدفع الإلكتروني.

مجموعات فيسبوك المغلقة

ثمة ثلاثة أنواع من المجموعات في فيسبوك: المفتوحة والمغلقة والمخفية.

- يمكن العثور على المجموعات المفتوحة عبر البحث عنها في المنصة ويمكن لأي شخص الانضمام إليها.
- يمكن العثور على المجموعات المغلقة أيضًا عبر البحث عنها، ولكن يلزم المستخدم طلب الانضمام إليها.
- لا يمكن العثور على المجموعات المخفية عبر البحث عنها في المنصة، ولا يمكن الانضمام إلى مثل هذه المجموعات إلى عبر دعوة خاصة.

ويتزايد إقبال الناس على المجموعات في فيسبوك، ويعود ذلك في جزء منه إلى خوارزميات المنصة نفسها والتي تشجع الناس على الانضمام

إلـى المجموعـات، لكـن الدافـع الأكبـر يتمثـل فـي الرغبـة المتزايـدة لـدى المسـتخدمين للتفاعـل مـع أشـخاص يرتبطـون معهـم بمعرفـة شـخصية أو اهتمام أو وجهة نظر مشتركة.

منصة "ديسكورد"

وفقًـا للأرقـام التـي أوردهـا موقـع "ستاتيسـتا" فـي يوليـو 2019، فقـد بلـغ عـدد المسـتخدمين النشـطين لمنصـة "ديسـكورد" 250 مليـون مسـتخدم (قارن ذلـك بتطبيـق سـناب بحوالـي 294 مليـون مسـتخدم، وفايبـر 260 مليـون، وتليغـرام 200 مليـون). ولتطبيـق ديسـكورد أفضليـة خاصـة لـدى مجتمـع الألعـاب الإلكترونيـة، ولكنـه بـات معروفًـا كمنصّـة يتجمـع فيهـا البعـض ضمن "خوادم" (أو مجموعات) لتنسيق حملات لنشر المعلومات المضللة.

ويلاحـظ فـي ديسـكورد وبعـض مجموعـات فيسـبوك المغلقـة طلـب الإجابـة علـى بعـض الأسـئلة كشـرط لقبـول انضمامـك إليهـا، وقـد تكـون هـذه الأسـئلة متعلقـة بطبيعـة عملـك، أو ديانتـك، أو توجهاتـك السياسـية، أو وجهـة نظـرك بشأن قضايا اجتماعية معينة.

التشفير والمجموعات والقنوات

أحـد الأسـباب التـي عـززت رواج هـذه المنصـات والتطبيقـات هـو أنهـا توفـر مسـتويات مختلفـة مـن "التشـفير". ويعـد واتسـاب وفايبـر حاليًـا الأكثـر موثوقية علـى مسـتوى التشـفير، وذلـك للاعتمـاد فيهمـا علـى آلية التشـفير بيـن الطرفيات (End to End). أمـا تليغـرام وفيسـبوك ماسـنجر ولايـن فـلا توفّـر خاصيـة التشـفير إلا فـي حـال تفعيلهـا. وثمـة تطبيقـات تتضمـن مجموعـات أو قنـوات تتيـح إمكانيـة مشـاركة المحتـوى مـع أعـداد ضخمـة مـن النـاس. الحـدّ الأقصـى لمجموعـات واتسـاب هـو 256 مسـتخدمًا، أو مجموعـات فيسـبوك ماسـنجر فتسـمح بإضافـة 250 شـخصًا فقـط. أمـا فـي تليغـرام، فقـد تكـون المجموعـات

خاصـة أو عامّـة، ويمكـن أن تضـم 200 مسـتخدم كحـدّ أقصـى، لكـن يمكن بعد تجـاوز هـذا الرقـم تحويلهـا إلـى "مجموعـة فائقـة"، وعندهـا يمكـن أن تضـمّ أكثـر مـن 75 ألـف مسـتخدم. كمـا يتوفـر فـي تليغـرام خاصيـة القنـوات، والتـي توفـر إمكانيـة نشـر المحتـوى داخـل التطبيـق، بحيث يمكن للمسـتخدم الاشـتراك فـي هـذه القنـاة والاطـلاع علـى المحتـوى الـذي يتـم نشـره عليهـا، ولا تكـون لـه القدرة على النشر أو التعليق.

المتابعة المستمرة

لا شـكّ فـي أن المعلومـات الزائفـة أو المضللـة تنتشـر فـي تطبيقـات المحادثـة المغلقـة، ويصعـب التقييـم بشـكل دقيـق إن كانـت هـذه التطبيقـات تشـتمل علـى قـدر أكبـر مـن المعلومـات الزائفـة مقارنـة بمـا هـو موجـود علـى مواقـع التواصـل الاجتماعـي نفسـها؛ وذلـك لأنـه يسـتحيل رؤيـة مـا يتشـاركه النـاس فيمـا بينهـم علـى تلـك التطبيقـات المغلقـة. لكننـا نـدرك أنهـا تمثّـل تحديًـا كبيرًا، وهـذا مـا تثبتـه العديـد مـن الحـالات والحـوادث المتعلقـة بالمعلومـات الزائفـة علـى تطبيقـات المحادثـة مـن دول مختلفـة كالهند وفرنسـا وإندونيسـيا وغيرها. فـي الولايـات المتحـدة وأثنـاء حادثتَـي إطـلاق النـار فـي إل باسـو ودايتـون فـي أغسـطس 2019، انتشـرت العديـد مـن الشـائعات والأخبـار المغلوطـة علـى تليغرام وفيسبوك ماسنجر.

والسـؤال المطـروح هـو مـا إذا كان علـى الصحفييـن والباحثيـن والعامليـن فـي مجـال التحقـق أو القطـاع الصحـي أو الناشـطين فـي مجـال العمـل الإنسـاني أن ينضمـوا إلـى مثـل هـذه المجموعـات المغلقـة للوقـوف علـى المعلومـات الزائفـة التـي قـد تنتشـر فيهـا. وفـي حـال التحاقهـم بمثـل هـذه المجموعـات، فبـأي صفـة سـيقدمون أنفسـهم، ومـا الوسـيلة التـي تراعـي الجانـب الأخلاقـي من جهة، ولا تعرّضهم إلى المخاطرة من جهة أخرى؟

وبالرغـم مـن التحديـات الجسـيمة المتوقعـة، إلا أنّ ذلـك ممكـن. لكـن عليـك أولًا أن تتذكـر أن العديـد مـن المسـتخدمين الذيـن يلجـؤون إلـى مثـل هـذه

التطبيقات والمجموعات إنما يفعلون ذلك لأنهم يرغبون في تجنب المراقبة، ولأنهم حريصون على استخدام أدوات تواصل مشفرة وآمنة وفيها مستوى معقول من الخصوصية. ويجدر بكل شخص يرغب في دخول هذه المساحات لأغراض عملية أن يدرك هذا الأمر، بالإضافة إلى ضرورة التعامل بمسؤولية تجاه المستخدمين في هذه المجموعات وخصوصيتهم.

أساليب البحث في المجموعات

ليس من السهل البحث عن هذه المجموعات والوصول إليها، إذ عادة ما تكون هنالك بروتوكولات محددة لكل منها. في فيسبوك، يمكن البحث عبر الموضوعات، ثم اختيار فلتر المجموعات. كما يمكن استخدام آلية بحث أكثر تقدمًا، عبر البحث في جوجل باستخدام الكلمات المفتاحية المطلوبة ثم إضافة صيغة: site:facebook.com/groups

أما في تليغرام، فيكمن البحث في التطبيق نفسه إن كنت تستخدم هاتف أندرويد، وليس ذلك متاحًا على هواتف الآيفون. ويمكن البحث فيها كذلك عبر تطبيقات سطح المكتب مثل https://www.tele-gram-group.com/. نفس الأمر بالنسبة لديسكور هناك موقع مثل https://disboard.org/search.

القرارات بخصوص الانضمام والمشاركة

أشرنا من قبل إلى أن بعض هذه المجموعات سيطرح بعض الأسئلة التي تكون الإجابة عليها شرطًا للانضمام إليها. وعليك قبل الإجابة عنها أن تستشير المحرر المسؤول أو المدير في المؤسسة التي تعمل لديها عن الطريقة الأسلم للإجابة عن هذه الأسئلة. هل عليك أن تكشف عن هويتك وعن سبب رغبتك في الانضمام للمجموعة؟ هل ثمة طريقة للانضمام وتعمُّد

أن تكون غامضًا؟ وكيف يمكن أن تسوّغ قرارك بشأن إخفاء هويتك الحقيقية (وهو أمر قد يكون مطلوبًا في حال كان الانضمام لمجموعة ما يشكّل خطرًا على أمنك الشخصي لو عرّفت عن نفسك بوصفك المهني كصحفي). وفي حال انضمامك للمجموعة المطلوبة، فهل ستكون عضوًا فاعلًا بالمشاركة والتعليق، أم ستبقى تترصّد المعلومات التي تسعى إلى ملاحظتها؟

جمع المحتوى بشكل آلي من داخل المجموعات

من الممكن تحديد المجموعات "المفتوحة" عبر البحث عن روابط تم نشرها لمواقع أخرى، والتي ستظهر بعدها في محركات البحث. وعليه فإنه من الممكن استخدام طرق آلية لجمع المحتوى بشكل آلي في حال ظهوره في هذه المجموعات. وقد قام بعض الباحثين أثناء عملهم على مراقبة الانتخابات في البرازيل والهند باستخدام هذه الطريقة، وأعرف بشكل شخصي بعض المؤسسات الأخرى التي قامت بذلك.

يساعد هذا الأسلوب على مراقبة عدة مجموعات معًا، وهو ما قد يكون القيام به يدويًا أمرًا مستحيلًا عادة. لكن تلزم الإشارة هنا إلى أنه لا يمكن العثور إلا على نسبة قليلة من المجموعات بهذه الطريقة، وهي عادة المجموعات التي يكون اهتمامها الأول جمع أكبر قدر من الأعضاء. كما أن هذه الطريقة ليست بلا محاذير أخلاقية، بالرغم من وجود ضوابط لها عبر تشفير البيانات وعدم مشاركتها مع أطراف أخرى ونزع التعريف عن الرسائل. ولا تزال ثمة حاجة إلى تطوير بروتوكولات مهنية خاصّة لضبط مثل هذا النوع من الأنشطة.

طلب الحصول على المعلومات

أما الأسلوب الآخر فهو التوجّه إلى العامة بشكل مباشر لطلب المعلومات والمحتوى، ويكون ذلك بتوجيه دعوة واضحة وبسيطة مع بيان هدفك من

الحصـول علـى هـذه المعلومـات وكيـف سـتقوم باسـتخدامها. فهـل الهـدف مجـرد مراقبـة المواضيـع الرائجـة فـي هـذه المجموعـات، أم أنـك تسـعى إلـى تفنيد بعض المعلومات الزائفة التي تعتقد أنها منتشرة فيها؟

ونعـود هنـا إلـى المسـألة الأخلاقيـة، والتـي يتـم اسـتدعاؤها بشـكل خـاص عنـد التعامـل مـع تطبيقـات المحادثـة. فـلا بـد مـن توضيـح أنـك لا تقـوم بجمـع المحتـوى وحسـب. وحتـى لـو حيّدنـا سـؤال الأخـلاق قليـلًا، فـإن الأبحـاث تظهـر مـن الناحيـة العمليـة أن العامـة الذيـن لا يمتلكـون فكـرة واضحـة عـن الكيفيـة التـي سـيتم بهـا اسـتخدام المحتـوى الـذي يقدّمونـه للصحفـي سـيكفّون بعـد فتـرة قصيـرة عـن التعـاون معـه، فـي حيـن سـيكون تعاونهـم أكبـر فـي حال شعروا أنه يتعامل معهم كشركاء.

لا بـدّ كذلـك مـن التنبـه إلـى سـهولة التلاعـب بهـذا المحتـوى الـذي يتطـوّع البعـض لإرسـاله، كأن يقـوم أحدهـم مثـلًا بإرسـال محتـوى مزيـف لـم يظهـر فـي أي مجموعـة، أو أن يقـوم مـع مجموعـة أخـرى مـن الأشـخاص بإرسـال نفـس المحتـوى بشـكل متكـرّر ومقصـود، فيتشـكل لـدى الصحفـي انطبـاع بـأن المشكلة أكبر مما هي عليه في واقع الأمر.

أخلاقيات إعداد التقارير بالاعتماد على رسائل مجموعات خاصة

عنـد العثـور علـى المحتـوى المطلـوب يبـرز سـؤال التعامـل معـه وكيفيـة الإشـارة إليـه. هـل يجـب الالتـزام بالشـفافية والإفصـاح عـن الكيفيـة التـي اتبعتها للحصول على المحتوى؟

بعـض المجموعـات تطلـب مـن أعضائهـا بشـكل واضـح فـي قواعدهـا الإرشـادية عـدم نشـر مـا يتـم نقاشـه داخـل المجموعـة. وإذا كانـت المجموعـة حقًّـا تشـتمل علـى قـدر كبيـر مـن المعلومـات الزائفـة أو المضللـة، فمـا الأثـر الـذي سـيترتب علـى المجموعـة فـي حـال إعـدادك تقريـرًا يتحـدث عـن المحتـوى الـذي يتداولـه أعضاؤهـا؟ هـل يمكـن أن يكـون هـذا المحتـوى

منتشرًا في غيرها من المجموعات أو المنصات الرقمية؟ وفي حال نشر التقرير الذي أعددته، هل سيمثل ذلك خطرًا على سلامتك أو سلامة زملائك أو أفراد أسرتك؟ تذكّر أيضًا أن الاختراق السيبراني للصحفيين والباحثين أسلوب انتقامي لن تتورّع بعض الجهات عن استخدامه.

خاتمة

إعداد التقارير الصحفية عن محتوى متداول داخل مجموعات أو تطبيقات محادثة مَهمة مليئة بالتعقيدات والتحديات، لكن هذه المساحات ستزداد أهمية بشكل متسارع مع اتساع دورها وتأثيرها كمصادر للمعلومات ومشاركتها.

علينا التفكير كخطوة أولى بشأن الأسئلة التي طرحناها في هذا الفصل، والحديث بشكل صريح مع الزملاء والمحررين المسؤولين. وإن لم يكن لدى الجهة التي تعمل لصالحها إرشادات تتعلق بهذا الجانب فمن الضروري التفكير بالاتفاق على بعض الإرشادات والمبادئ العامة الموجِّهة للعمل مع هذه التطبيقات. ليس ثمّة قواعد معيارية تصلح لكل حالة؛ فلكل قصة صحفية اعتباراتها المتعلقة بالموضوع وبالمنصة والصحفي نفسه وبالقواعد المعمول بها في المؤسسة، ومن الضروري أن نأخذ بالحسبان كافة التفاصيل الضرورية قبل الشروع بالعمل.

دراسة حالة: بولسونارو في المستشفى

سيرخيو لودتكا

سيرخيو لودتكا صحفي ومحرر في مؤسسة "Projeto Comprova"، وهو تحالف من 24 مؤسسة إعلامية تتعاون معًا للتصدي للشائعات حول السياسات العامة في البرازيل والتحقق منها، وقد عملت في العام 2018 على مراجعة المحتوى المشبوه الذي انتشر على شبكات التواصل الاجتماعي وتطبيقات المحادثة في فترة الانتخابات الرئاسية في البرازيل.

في 6 سبتمبر 2018 قبل شهر على موعد الانتخابات الرئاسية في البرازيل، شارك المرشح الرئاسي اليميني خايير بولسونارو في مهرجان انتخابي في مركز المدينة في خويز دي فورا، وهي مدينة يقطنها حوالي 560 ألف نسمة وتبعد 200 كم عن ريو دي جانيرو.

كان قد مضى أسبوع واحد فقط على تصدّر بولسونارو في استطلاعات الجولة الأولى للانتخابات الرئاسية في البرازيل، وقد حصل ذلك بعد أن أعلنت المحكمة الانتخابية العليا قرارها في عدم قبول ترشح الرئيس السابق لويس إيناسيو لولا دا سيلفا.

لكن هذا لم يكن يعني أن بولسونارو يمتلك فرصًا مؤكدة للفوز، فمنافسوه الثلاثة الآخرون كانوا يحققون نتائج متقدمة في الاستطلاعات.

لقد كان موقف بولسونارو صعبًا؛ إذ لم يكن لديه سوى فسحة دعائية مجانية من 9 ثوان فقط على التلفاز. فبحسب القوانين الناظمة للانتخابات

في البرازيل، تمنح محطات الراديو والتلفزيون وقتًا حرًّا للأحزاب السياسية للترويج لبرامجهم الانتخابية، بحيث يتم توزيع هذا الوقت بحسب عدد المقاعد التي فاز بها كل حزب في الانتخابات الأخيرة لمجلس النواب. وقد كان غياب المقاعد لبولسونارو مأزقًا من هذه الناحية، فقد عنى ذلك أنه لا يملك سوى ثوان معدودة للترويج لحملته على وسائل الإعلام المحلية، وقد اعتمد بدل ذلك على أنصاره على شبكات التواصل الاجتماعي، وكثف من اختلاطه المباشر مع الناس في الشوارع والأحياء.

في خويز دي فورا وغيرها من المدن التي زارها من قبل، شارك بولسونارو في مسيرة حُمل بها على أكتاف أنصاره وساروا به مبتهجين، إلى أن حصل تحوّل مفاجئ في المشهد. تقدّم أحدهم بين الجموع وحاول طعن بولسونارو، وغرز السكين في بطنه، ما أدى إلى تفجّر الجدل على وسائل التواصل الاجتماعي.

انتشرت الشائعات ونظريات المؤامرة، فتارة تبرز ادعاءات باتهام الرجل الذي طعن بولسونارو بأن له علاقات مع حزب الرئيس الأسبق ديلما روسيف، والذي عزل من منصبه عام 2016، وتارة تنتشر صور مفبركة يظهر فيها المهاجم إلى جانب لولا دا سيلفا، واتهمه البعض بأنه ينتمي إلى حزب "الاشتراكية والحرية" (PSOL) اليساري، وزاد محاموه طين الشائعات بلّةً حين رفضوا الإفصاح عن الجهة التي تدفع لهم أتعابهم.

في الوقت ذاته حققت مقاطع الفيديو والرسائل الداعمة لبولسونارو زخمًا كبيرًا على منصات التواصل الاجتماعي، رغم انتشار محتوى آخر يدّعي أن الهجوم مفبرك، وأن بولسونارو في المستشفى لتلقي العلاج من السرطان، وأن الصور التي انتشرت عن عمليته الجراحية محض فبركة.

لقد كانت عملية الطعن كفيلة بإعلان بولسونارو إيقاف أنشطته الجماهيرية، ولكن العملية ضمنت لها تفوقًا معقولًا في الاستطلاعات، وانتهت الانتخابات كما هو معروف بفوزه.

في 19 سبتمبر، أي بعد أسبوعين تقريبًا من الهجوم، تعقبت أداة (Eleições sem Fake)، وهي برنامج مراقبة لمجموعات واتساب من إنشاء جامعة ميناس غيرايس (Minas Gerais)، مقطعًا صوتيًا تم تداوله على قطاع واسع، وانتشر في 16 مجموعة من أصل 300 مجموعة يراقبها البرنامج، وبعضها كانت محسوبة على أنصار بولسونارو. في اليوم ذاته تلقت المؤسسة التي أعمل بها طلبات من القراء عبر تطبيق واتساب أيضًا بالتحقق من صحة التسجيل.

في التسجيل الذي بالكاد تجاوز الدقيقة ظهر صوت رجل مماثل لصوت بولسونارو يتجادل مع شخص يبدو أنه ابنه، ادواردو، ويشتكي من أنه لا يستطيع مغادرة المستشفى، وقال في التسجيل إنه لم يعد قادرًا على احتمال "هذه المسرحية"، ما يشير إلى أن الحادثة كلها مختلقة.

في ذلك اليوم، كان بولسونارو ما يزال على سرير العلاج في وحدة العناية شبه المركزة في مستشفى ألبرت أينشتاين في ساو باولو. التقرير الطبي الخاص به يفيد بأنه لا يعاني من الحمّى، وأنه يحصل على التغذية عبر الوريد، وأنه استعادة عافية أمعائه.

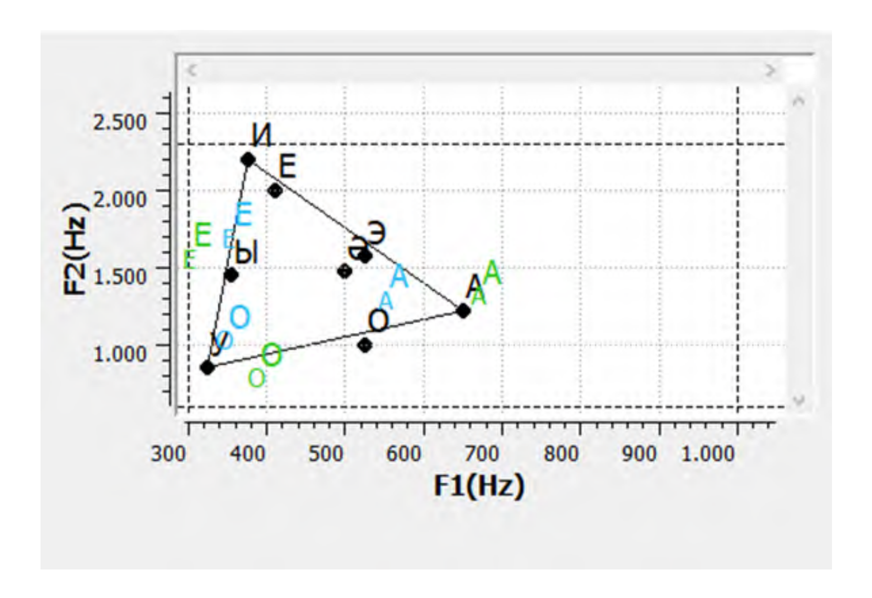
لم تتمكن مؤسسة كومبروفا من التوصل إلى المصدر الأصلي للتسجيل الذي انتشر بشكل أساسي عبر واتساب، في وقت كان ما يزال من الممكن فيه مشاركة الملفات في 20 محادثة، ما يضمن سرعة انتشار المحتوى، والذي سرعان ما يصل أيضًا إلى وسائل التواصل الاجتماعي الأخرى، وبات من المستحيل تعقب الملف إلى مصدره الأصلي.

وفي ظل تلاشي إمكانية تحديد المصدر الذي أنشأ التسجيل، عمدت مؤسسة كومبروفا إلى أساليب تقليدية أكثر في التحقق، وطلبت مساعدة بعض الخبراء من المعهد البرازيلي للتحليلات الجنائية، والذين توصلوا بعد مقارنة الصوت الوارد بالتسجيل مع صوت بولسونارو في إحدى المقابلات معه في أبريل 2018 إلى أن الصوتين مختلفان وأن التسجيل الذي جرى تداوله على نطاق واسع على وسائل التواصل الاجتماعي

ليس صادرًا عن بولسونارو.

اعتمد الخبراء على عملية تحليل نوعيةٍ للصوت والنطق والعلامات اللغوية الواردة في التسجيل ومقارنتها مع العيّنات الصوتية المتوفرة لديهم. وقد تضمن هذا التحليل مراقبة الأنماط في نطق الحروف الصامتة والصائتة، ونغمة الحديث وسرعته، وطبقة الصوت وجودته والعادات اللغوية لدى المتحدث، إضافة إلى استخدام بعض الكلمات والتراكيب النحوية المحددة.

يظهر في الصورة أدناه تحليل التكرار للمكوّنات الإصغائية في الكلام "Formants"، والنغمات الناتجة عن اهتزازات التجويف الصوتي حيث تجري فلترة الأصوات التي يتم إنتاجها في الحنجرة. فالهواء داخل التجويف الصوتي يهتز بنغمات ذات مستويات مختلفة بالاعتماد على بعض العوامل. في هذا الشكل يتم تحليل المكوّنات الإصغائية تكراريًا عبر التركيز على الحروف الصائتة "A" و "E" و "O". الصوائت باللون الأخضر تتوافق مع عينة التسجيل الصوتي الذي انتشر عبر واتساب، أما التي باللون الأزرق فتتوافق مع العينة الصوتية من مقابلة بولسونارو قبل أيام من الهجوم.



وقد كشفت المزيد من التحليلات أن كلام المتحدث في التسجيل المتداول يتضمن مؤشرات على لهجة سائدة في أرياف ساو باولو، وهي ملاحظة لم تظهر في أنماط حديث بولسونارو التي خضعت للتحليل، هذا بالإضافة إلى فروقات في رنّة الكلام والنطق وسرعته والانحرافات الصوتية بين العينتين.

ولمزيد من التأكّد استعانت مؤسسة كومبروفا بخبير آخر، وقد توصل هو الآخر إلى أن الصوت في التسجيل يختلف عن صوت بولسونارو لعدّة أسباب، من ضمنها ما لاحظه من حدّة النغمة المرافقة للنطق في تسجيل واتساب مقارنة بالعينات المتوفرة لكلام بولسونارو، إضافة إلى سرعة النطق والتي بدت أعلى في التسجيل مقارنة بعينة من مقطع فيديو سجّل لبولسونارو وهو في المستشفى.

ومما أكّد أيضًا أن المقطع الصوتي المتداول مفبرك هو رداءة جودة التسجيل. فقد أشار بعض الخبراء المختصين إلى أن هذه حيلة رخيصة شائعة، إذ يجري التلاعب بشكل مقصود بدقّة التسجيلات الصوتية أو مقاطع الفيديو أو الصور وذلك بهدف زيادة الصعوبة في تحليلها.

أما على صعيد ردّة الفعل، فقد ظهر نجلا بولسونارو، فلافيو وكارلوس، في مقطع مصور على وسائل التواصل الاجتماعي ليؤكدا أن التسجيل "أخبار زائفة".

لو كان ذلك التسجيل انتشر في وقتنا الحالي، لما استطاع أن يدفع هذا القدْرَ من الناس إلى التصديق بأنه عائدٌ حقًّا لبولسونارو. ففي الفترة التي انتشر فيها المقطع لم يكن صوت بولسونارو مسموعًا ومألوفًا في وسائل الإعلام بتلك الثواني المعدودة المخصصة لحملته الانتخابية على وسائل الإعلام العامة، إضافة إلى توقف مشاركته في المهرجانات الانتخابية والمناظرات بعد دخوله المستشفى وتلقيه العلاج. وقد خلق ذلك فرصةً لانتشار ذلك التسجيل المفبرك الذي تسبّب بخداع الكثيرين.

بعد أكثر من عام على تلك الحادثة، ما يزال يصعب معرفة السبب الذي جعل جماعات مناصرة لبولسونارو ومشاركة في حمَلاته الانتخابية تقوم بترويج ذلك التسجيل الذي كان كفيلًا بتدمير فرَصه بالفوز في الانتخابات لو ثبتت صحته، ولن يتسنّى لنا غالبًا تفسير ذلك الاندفاع بين تلك المجموعات لمشاركته وترويجه. لكن ما يهمنا في النهاية هو تذكّر هذه الحادثة كمثال جليّ على قدرة محتوى بهذا القدر من الحساسيّة على الانتشار بتلك السرعة المرعبة على وسائل التواصل الاجتماعي.

الفصل الثامن: التحقق من المواقع الإلكترونية

كريج سيلفرمان

كريغ سيلفرمان هو محرر الوسائط الإعلامية في موقع -Buzz Feed News، وهو مسؤول عن فريق عالمي لمتابعة المنصات، والمعلومات المضللة، وحملات التضليل على وسائل الإعلام. سيلفرمان عمل على تحرير "دليل التحقق" و"دليل التحقق للصحافة الاستقصائية"، وهو مؤلف كتاب بعنوان (Lies, Damn Lies, and Viral Content: How News Websites Spread (and Debunk) Online Rumors, Unverified Claims and Misinformation).

تستخدم المواقع الإلكترونية من قبل المنخرطين في حملات التضليل الإعلامي من أجل كسب الإيرادات وتجميع عناوين البريد الإلكتروني وغيرها من المعلومات، أو من أجل توظيفها كنقاط لتجميع المحتوى المضلل. ويجدر بالصحفيين امتلاك القدرة على التحقق من الأنشطة على المواقع الإلكترونية، والكشف عن أي علاقات ممكنة مع عمليات أكبر تعتمد على حسابات على منصات التواصل الاجتماعي، أو تطبيقات، أو شركات، أو غير ذلك.

ومن الضروري أن نتنبّه إلى أن النصوص أو الصور أو حتى المواقع نفسها التي نقوم بمراقبتها قد تختفي مع الوقت، خاصة بعد محاولة الصحفي التواصل مع الأشخاص المرتبطين بها وطرح الأسئلة عليهم. لذا فإن أفضل الممارسات المعتمدة تشتمل على استخدام أداة "-Way Back Machine" من أجل حفظ الصفحات المهمة على الموقع

الإلكتروني موضوع التحقق بحيث يكون ذلك جزءًا أساسيًا من سير العمل. وفي حال مواجهة صعوبة في حفظ صفحات معينة باستخدام هذه الأداة، فيمكن استخدام أداة أخرى مثل archive.today. هذا يضمن للصحفي أن يربط هذه الصفحات المؤرشفة كدليل على ما توصّل إليه من نتائج، مع تجنب الربط المباشر مع الموقع الذي ينشر المعلومات الزائفة و/أو المضللة.

وتعد أداة Hunchly من أفضل الأدوات المدفوعة لإنشاء أرشيف خاص بصفحات الويب التي تعمل على فحصها، بحيث يتم حفظ الصفحات تلقائيًّا أثناء العمل. هذه الأدوات الخاصة بالأرشفة مهمة كذلك في تتبع شكل الموقع خلال فترة من الوقت، وأنصح بشكل خاص بتنصيب أداة Wayback Machine المتوفرة كإضافة على المتصفح، ما يسهّل عملية أرشفة الصفحات وتتبع النسخ السابقة وفحصها.

إضافة أداة Ghostery على المتصفح مفيدة كذلك في معرفة أدوات التتبع (Trackers) على موقع إلكتروني ما، مثل تحديد ما إذا كان الموقع يستخدم أداة "جوجل أنالتيكس" و/أو "جوجل أدسنس"، وهو أمرٌ ضروري للمساعدة مع أساليب التحقق التي سنتطرق إليها فيما يلي.

سيتطرق هذا الفصل إلى أربعة جوانب للتحليل في سياق التحقق من المواقع الإلكترونية وهي: المحتوى، وكود الموقع، وأدوات التحليل، والتسجيل والعناصر الأخرى المرتبطة بالموقع.

المحتوى

معظم المواقع الإلكترونية تعطيك نبذة مهما كانت صغيرة عن طبيعتها، سواء كان ذلك عبر قسم تعريفي خاص على الموقع، أو وصف في الصفحة الرئيسية في الهامش أو أي مكان آخر. وهذه نقطة بداية جيدة. فغياب مثل هذه المعلومات التعريفية في الموقع الإلكتروني يعني أن

الموقع قد أنشئ على عجل، أو أن من أنشأه حريص على التعمية على هدفه أو الجهة التي تقف وراءه.

وإلى جانب الاطلاع على أي تعريف ذاتي عن الموقع، في قسم "من نحن" أو غيره، فمن الضروري التصفح العام لمحتوى الموقع؛ سعيًا إلى تحديد أي مؤشّر قد يدلُّ على الجهة المسؤولة عن تشغيله، وأهدافه، وما إذا كان جزءًا من شبكة أو مشروع أكبر. ومن الضروري التنبه إلى العناصر التالية:

- هل توجد إشارة إلى صاحب الموقع أو أي شركة يتبع لها؟ هل يوجد قسم "من نحن" في الموقع؟
- هل توجد إشارة إلى شركة أو شخص في القسم الخاص بحقوق النشر في أسفل الصفحة الرئيسية أو أي صفحة أخرى؟
- هل يتم ذكر أي أسماء أو عناوين أو أسماء شركات في القسم الخاص بسياسة الخصوصية أو الأحكام والشروط؟ هل هذه الأسماء أو الشركات تختلف عما يكون قد ورد في ذيل الصفحة، أو في قسم "من نحن" أو غيرها من الأقسام على الموقع؟
- لاحظ في حال كان الموقع ينشر مقالات إن كان ثمة روابط في داخلها تحيل إلى نبذة عن الكاتب أو إلى حساباته على وسائل التواصل الاجتماعي.
- هل يرتبط الموقع بحسابات رسمية على مواقع التواصل الاجتماعي؟ يمكن البحث عن الأيقونات الصغيرة الخاصة بمنصات التواصل الاجتماعي في أسفل الصفحة الرئيسية أو أعلاها أو في مكان آخر. وفي حال وجدت ذلك، حرك المؤشّر فوق هذه الأيقونات، وانظر إلى الطرف السفلي على يسار نافذة المتصفح، وتنبّه إلى الرابط الذي تؤدي إليه. في بعض الحالات يتم إنشاء بعض المواقع على عجل، دون الاهتمام بوضع الروابط الصحيحة في الأماكن المطلوبة ضمن القالب المستخدم، ولذا قد تجد أن الرابط يؤدي إلى منصة فيسبوك وحسب، وليس إلى صفحة خاصة بالموقع.

- هل يتحدث الموقع عن منتجات أو عملاء أو شهادات أو شركات قد يكون مرتبطًا بها؟
- احرص على التنقيب في الموقع الإلكتروني جيدًا بدل الاكتفاء بالنظر إلى الصفحة الرئيسية. تفحَّصْ كافة القوائم والأقسام التي تشتمل عليها، وتفحص الصفحات من الأعلى إلى الأسفل؛ للعثور على أي معلومات أو روابط أو صفحات قد تساعدك زيارتها على معرفة المزيد من المعلومات عن الموقع.

من أهم النقاط المتعلقة بتفحص محتوى الموقع هو الحكم عليه إن كان أصليًا أو لا. هل تم نسخ النص الموجود في قسم "من نحن" من موقع آخر؟ هل يوجد أي محتوى آخر منسوخ من مواقع أخرى؟ هل يتضمن الموقع محتوى مضللًا أو مزيفاً؟ أو هل يدلّ على دعم واضح لأجندة معينة؟

أُجريت في العام 2018 عملية تحقق للكشف عن مخطط احتيال ضخم في مجال الإعلانات الرقمية، تضمّن الاستعانة بتطبيقات على الهواتف النقالة ومواقع إلكترونية مختصة بنشر المحتوى، إضافة إلى شركات وهمية وشركات تمويه، وموظفين وهميين. وتمكنتُ في نهاية التحقيق أن أكشف عن أكثر من 35 موقعًا إلكترونيًا مرتبطًا بذلك المخطط. ومن الطرق التي اتبعتها لاكتشاف زيف تلك المواقع كانت عبر نسخ النص في قسم "من نحن" والبحث عنه في جوجل، فوجدت أن النص مشتركٌ حرفيًا في حوالي 20 موقعًا.



كما أنشأ المحتالون الذين حاولوا تدبير تلك العملية مواقع إلكترونية لشركات التمويه التي يدّعون امتلاكها، وذلك كي يُعطوا انطباعًا واثقًا أمام شركائهم المحتملين عند زيارة هذه المواقع الإلكترونية للتحقق منها.

أحد الأمثلة كان لشركة تُدعى Atoses، والتي أدرجت على الصفحة الرئيسية لموقعها الإلكتروني قائمة بأسماء عدد من كبار الموظفين لديها وصورهم الشخصية. لكن وعبر عملية بحث عكسي عن الصور على أداة Yandex تبين أن العديد من هذه الصور كانت صورًا تجاريّة تمّ الحصول عليها من مواقع بيع الصور على الإنترنت.



وفي ذيل الصفحة الرئيسية على الموقع تظهر للمتصفح هذه العبارة: "We craft beautifully useful, connected ecosystems that grow businesses and build enduring relationships between online media and users"، وتبين عبر البحث على جوجل أن النص نفسه مستخدم بشكل حرفيّ في مواقع تابعة لوكالتين إعلانيتين:

www.pimula.net › about-us ▾
About Us - Pimula Agency
Pimula is a fully integrated **digital** marketing agency that **crafts beautifully useful**, **connected digital ecosystems that grow businesses and build enduring relationships between** brands and humans. ... Thanks to the **connected** world, an idea in one continent could possibly mean a huge **business** in another.

www.netwyn.com ▾
Netwyn: Home
We craft beautifully useful, **connected ecosystems** that **grow businesses** and **build enduring relationships between** ... From designing websites to providing state **of** the art **digital** security, Netwyn is ... We host monthly networking events allowing you to meet with other like minded **business** people and **build** connections.

وعند ملاحظة أن الشركة استخدمت صورًا تجارية وادّعت أنها صور حقيقة لموظفيها، وعملت على سرقة نصّ تعريفي ونسخه على موقعها، فلا بدّ أن نفترض أنّها كذلك شركة وهميّة وأن الموقع واجهة للتمويه وحسب.

من الجيد كذلك البحث عبر محركات البحث باستخدام جمل من المقالات التي تظهر في المقالات المنشورة على الموقع، وذلك لمعرفة إن كان المحتوى مسروقًا من مواقع أخرى، فأحيانًا قد تجد الموقع الذي يدّعي أنه مصدر للأخبار أو المعلومات ينتحل المحتوى المنشور في مواقع أخرى.

في العام 2019، تفحصت موقعًا بعنوان Forbesbusinessinsider.com يدّعي أنه موقع إخباري مختص بقطاع التكنولوجيا، وتبيّن أنه يسرق المقالات بالجملة من مواقع أخرى. ومن المثير للسخرية أن أحد المقالات المسروقة هي مقالة لي كنت كتبتها بخصوص المواقع الإلكترونية المحلية المزيفة.

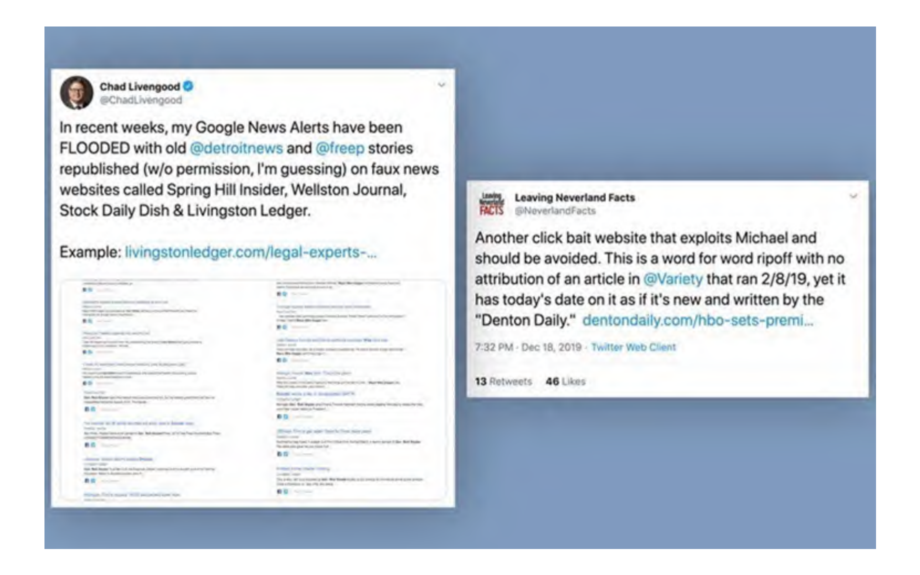
وثمة خطوة أساسية أخرى تتمثل في نسخ رابط الموقع والبحث عنه في جوجل. في المثال السابق (Forbesbusinessinsider.com)،

تساعدك هذه العملية على تقدير حجم الصفحات لهذا الموقع، كما يمكن أن تجد أشخاصًا آخرين بَلّغوا عن الموقع وحَذّروا من عمليات انتحال المحتوى التي يقوم بها.

يمكن كذلك أن تتأكد إن كان الموقع معترفًا به ضمن "أخبار جوجل"، وذلك عبر البحث في قسم "أخبار جوجل" باستخدام الرابط "Forbes-businessinsider" في صندوق البحث.

من الضروري أيضا البحث عن الرابط الخاص بالموقع في تويتر أو فيسبوك، وسيساعدك ذلك على تحديد ما إذا كان ثمّة أشخاص محدّدون مرتبطون بالموقع أو يحرصون على نشر محتواه.

في إحدى المرات تفحّصت موقعًا يدعى dentondaily.com، وظهرت على صفحته الرئيسية بعض المقالات التي نشرت مطلع العام 2020. لكن بعملية بحث بسيطة باستخدام عنوان الموقع على تويتر، اكتشفت وجود بعض الشكاوى والتعليقات التي تتهم الموقع بأنه ينتحل المحتوى. وبالرغم من أنّ المحتوى المذكور قد حذف من الموقع، إلا أن التغريدات التي كشفت ذلك الانتحال ظلت موجودة.



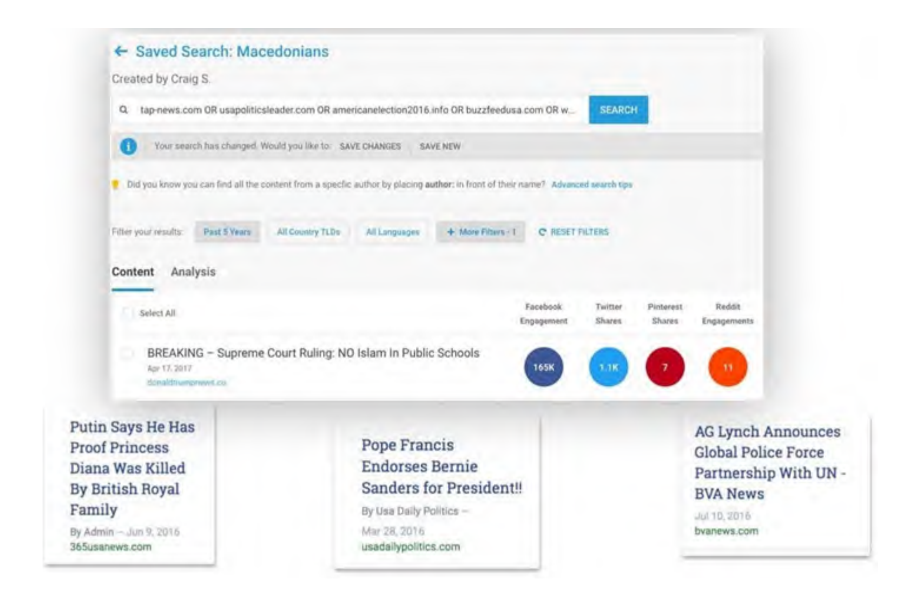
بعد التنقيب بما يكفي في محتوى الموقع، ننتقل إلى الخطوة التالية، والتي تتمثل في معرفة أنماط انتشار هذا المحتوى.

وللمساعدة في ذلك سنستعين بأداتين: BuzzSumo وCrowdTangle. في العام 2016، عملت مع الباحث لورنس أليكساندر للتحقيق في شأن بعض مواقع أخبار السياسة الأمريكية التي تدار من خارج الولايات المتحدة، وتوصلنا إلى عدد من المواقع التي تدار من مدينة فيليس شمال مقدونيا. وبالاعتماد على التفاصيل الخاصة بتسجيل اسم النطاق، اكتشفنا وجود أكثر من 100 موقع للأخبار السياسية الخاصة بالولايات المتحدة تدار من تلك المدينة الصغيرة.

كنت أود معرفة نوعية المحتوى الذي تنشره هذه المواقع ومدى رواجه، فنسخت عناوين عدد من هذه المواقع التي كانت أكثر نشاطًا، وشرعت بالتحري عنها في أداة BuzzSumo، وهي أداة توفر لك قائمة بمحتوى الموقع الذي حاز أعلى قدر من التفاعل على فيسبوك وتويتر وبنتيريست وريديت. (وللأداة نسخة مجانية، لكن النسخة المدفوعة تقدم نطاقًا أوسع من النتائج).

لاحظت مباشرة أن مقالات الموقع التي حازت أعلى قدر من التفاعل على فيسبوك كانت تتضمن محتوى مزيفًا، وقد كانت هذه الملاحظة أساسية لأنها حولت زاوية النظر للقضية مقارنة بالقصص الصحفية السابقة التي تناولت الموضوع.

الصورة أدناه تُظهر نتائج البحث التي حصلنا عليها في BuzzSumo، وفيها قوائم بالتفاعل الذي حصده أحد المواقع على فيسبوك وتويتر وبينتريست وريديت، إضافة إلى بعض القصص الصحفية الزائفة من العام 2016.



ومن الطرق الأخرى التي تُفيد في معرفة كيفية انتشار محتوى موقع ما على فيسبوك أو تويتر أو إنستغرام أو ريديت هي تنصيب أداة CrowdTangle المجانية كإضافة على المتصفح، أو عبر الموقع الخاص بالأداة على الشبكة، وكلتا الطريقتين تقدِّم نفس النتائج، ولكن الأمثلة التي سنستعرضها هنا تعتمد على نسخة الأداة على الموقع (هذه الأدوات مجانية، ولكن يلزمك حساب فيسبوك لاستخدامها).

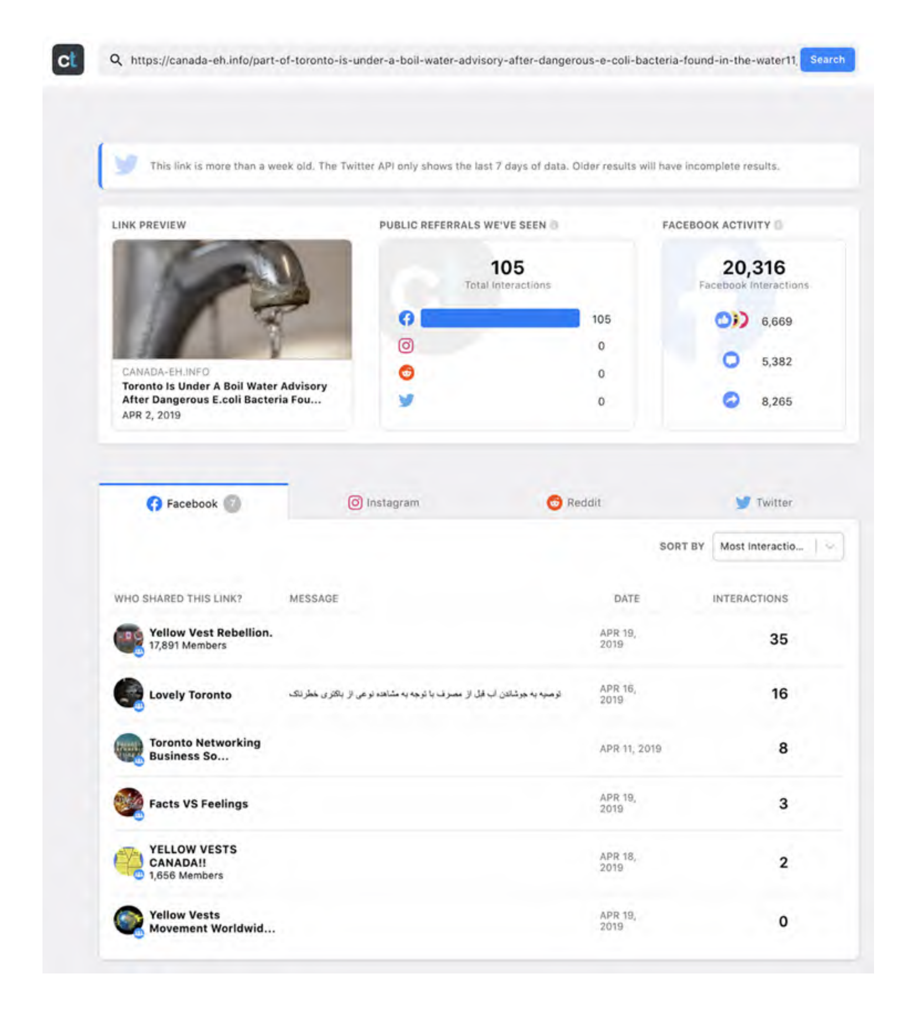
يكمن الفارق الأساسي بين BuzzSumo وCrowdTangle في إمكان استخدام الرابط الخاص بالموقع (URL) في BuzzSumo ليعرض لك تلقائيًا محتوى الموقع الذي نال أكبر قدر من التفاعل. أما في CrowdTangle فيتم استخدامها لفحص أداء رابط محدد داخل الموقع.

فلو بحثت مثلًا عن الرابط (buzzfeednews.com) باستخدام CrowdTangle فإن الأداة ستُظهر لك الإحصاءات الخاصة بالتفاعل مع الصفحة الرئيسية وحسب، أما لو أدخلت الرابط نفسه على BuzzSumo فستتمكن من معرفة المحتوى الأكثر رواجًا في الموقع عمومًا وليس أداء الصفحة الرئيسية فقط.

الفرق الآخر هو أن البحث عبر CrowdTangle سيقدم التفاعل على تويتر لفترة تغطي سبعة أيام فقط، أما BuzzSumo فتقدم رقم المشاركات على تويتر للمقالات التي يتضمنها الموقع.

استعنتُ مرة بأداة CrowdTangle للبحث عبر رابطٍ لقصة صحفية قديمة زائفة بخصوص اشتباه بحدوث تلوث في مياه الشرب في تورونتو (وقد حذف الموقع المقال لاحقًا لكن الرابط ما يزال فعالًا حتى لحظة كتابة هذا الفصل). وفقًا للنتائج التي ظهرت، فإن الرابط كان قد حصد 20.000 تفاعل وتعليق ومشاركة على فيسبوك منذ نشره.

كما يُظهر في النتائج بعض الصفحات والمجموعات العامة التي نشرت رابط المادة، إضافة إلى توفير خيار عرض النتائج الخاصة بالتفاعل على إنستغرام وريديت وتويتر، علمًا أن النتائج الخاصة بتويتر لا تُظهر سوى النتائج في الأيام السبعة السابقة لعملية البحث.



نلاحظ هنا أن العدد الكبير من مجموع التفاعلات التي حصدها الرابط ليس متوافقًا مع الأرقام المتواضعة التي تظهر في القائمة الخاصة بالصفحات والمجموعات؛ وهذا يعود في جزء منه على الأقل إلى أن أبرز الصفحات التي نشرت الرابط في البداية تعرضت للحذف لاحقًا من قبل فيسبوك.

لذا فإنه من الضروري أن نتنبّه إلى أن أداة CrowdTangle لا تَعرض سوى البيانات من الحسابات الفعالة، كما أنها لا تُظهر لك كل حساب عامّ قام بمشاركة الرابط. فما يظهر في النتائج عينة وحسب، ولكنها مع ذلك مفيدة جدًا، لأنها عادة ما تكشف عن ارتباط واضح بين حسابات محددة على وسائل التواصل الاجتماعي وموقع ما.

فإن كانت صفحة محددة ما على فيسبوك تنشر محتوى هذا الموقع بشكل مستمر أو حصري، فإن ذلك قد يكون مؤشرًا على أن الصفحة تابعة لنفس الجهة التي تدير الموقع. عندها سيكون عليك البحث بشكل أكبر في تلك الصفحة لتجد أي معلومات أخرى تربطها بالموقع، ولعلك تتمكن من تحديد هويات بعض الأشخاص ومعرفة دوافعهم.

كما قد تشتمل قائمة النتائج من CrowdTangle على حسابات لأشخاص شاركوا رابط المقال على إحدى المجموعات في فيسبوك، ويمكنك الاستفادة من هذه البيانات للتحري عن هذه الحسابات ومتابعة ما إذا كانت نشرت روابط أخرى من نفس الموقع، وقد يساعدك ذلك على التوصل لبعض النتائج.

التسجيل

كل اسم نطاق على الشبكة ينتمي إلى قاعدة بيانات مركزية تخزّن المعلومات الأساسية الخاصة بإنشاء الموقع وتاريخه. في بعض الحالات قد يحالفنا الحظ ونعثر على معلومات عن الشخص أو الشركة التي

دفعت لتسجيل اسم النطاق. ويمكن العثور على هذه المعلومات عبر بحث بسيط في أدوات عديدة مجانية.

يتوفر أيضًا عدد من الأدوات الأخرى المجانية أو الرخيصة التي يمكن الاستعانة بها للحصول على المزيد من المعلومات، مثل تحديد الأطراف التي تعاقبت على ملكية اسم النطاق، والخوادم التي يعتمد عليها الموقع، وغيرها من التفاصيل الأخرى المفيدة.

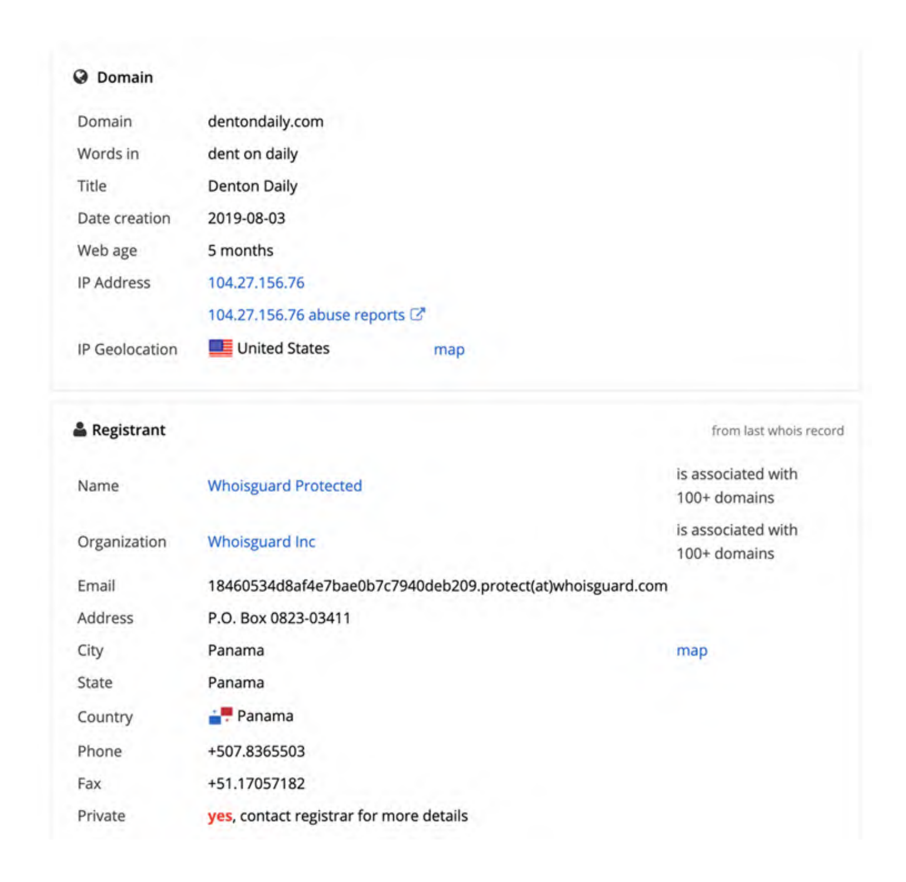
لكن لا بدّ من الإشارة هنا إلى أنّه يمكن ومقابل مبلغ بسيط إخفاء المعلومات الخاصة وحمايتها عند تسجيل اسم النطاق. فلو بحثت عن مثل هذه التفاصيل عبر الأدوات المختصة بذلك أثناء التحري عن موقع ما وكانت نتيجة البحث تَظهر لك عبارات من قبيل (Registration Private)، أو (WhoisGuard Protected) أو (Perfect Privacy LLC)، فهذا يفيد بأن معلومات التسجيل "محميّة". وحتى في هذه الحالات، فإن البحث عبر موقع (whois) سيقدم بعض المعلومات المتعلقة بتاريخ تسجيل اسم النطاق على الأقل، وموعد انتهائه وعنوان بروتوكول الإنترنت الخاصة باستضافة اسم النطاق.

ويعد موقع DomainBigData من أفضل الأدوات المجانية للتحقق من اسم النطاق وتاريخه. يمكن كذلك البحث في هذه الأداة عبر البريد الإلكتروني أو اسم شخص أو شركة، وليس عبر الرابط الإلكتروني للموقع فقط.

ثمة خدمات أخرى غير مجانية -ولكنها معقولة التكلفة- قد يلزمك كذلك الاطلاع عليها، من بينها (DNSlytics)، و(Security Trails)، و(Whoisology). منصة "آيريس" للتحقق التي يوفرها موقع Do-mainTools تعد من الخيارات الممتازة أيضًا، ولكنّها أعلى تكلفة.

لو بحثنا مثلًا عن موقع dentondaily.com على أداة DomainBig-Data فسنلاحظ أن بيانات التسجيل محميّة، وذلك لأنه يَظهر مكانَ اسم

الطـرف الـذي سـجّل النطـاق عبـارةُ "Whoisguard Protected"، لكـن المعلومـة التـي يمكـن أن نَخـرج بهـا مـن عمليـة البحـث -لحسـن الحـظ- هـو أن اسم النطاق قد سُجّل في تاريخ أغسطس 2019.



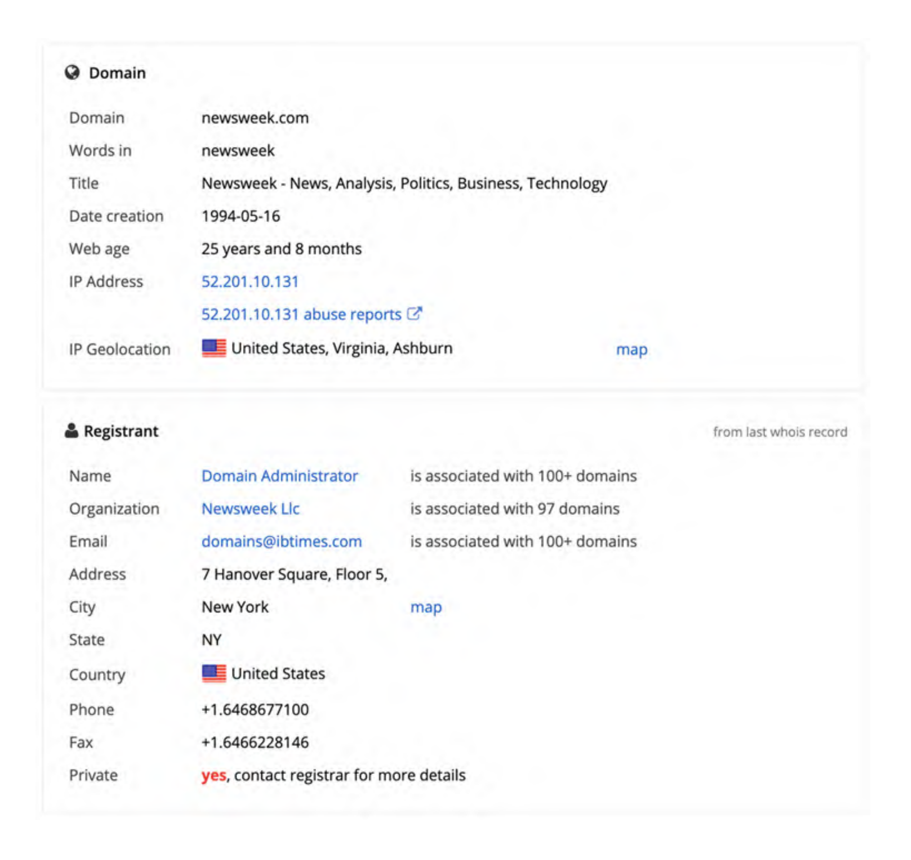
Domain

Domain	dentondaily.com
Words in	dent on daily
Title	Denton Daily
Date creation	2019-08-03
Web age	5 months
IP Address	104.27.156.76
	104.27.156.76 abuse reports
IP Geolocation	United States map

Registrant from last whois record

Name	Whoisguard Protected	is associated with 100+ domains
Organization	Whoisguard Inc	is associated with 100+ domains
Email	18460534d8af4e7bae0b7c7940deb209.protect(at)whoisguard.com	
Address	P.O. Box 0823-03411	
City	Panama	map
State	Panama	
Country	Panama	
Phone	+507.8365503	
Fax	+51.17057182	
Private	yes, contact registrar for more details	

ولـو بحثنــا مثـلًا عـن اسـم نطـاق newsweek.com عبـر الأداة ذاتهـا، فسـنلاحظ أن مالـك اسـم النطـاق لـم يدفـع لخدمـة حمايـة معلومـات التسـجيل، لذلـك يظهـر لدينـا اسـم الشـركة التـي اشـترت اسـم النطـاق، وعنـوان بريـد إلكتروني، ورقم هاتف وفاكس.



كما نلاحظ أن هذه الشركة هي مالكة اسم النطاق منذ مايو 1994، وأن الموقع حاليًا مرفوع على عنوان بروتوكول إنترنت رقم 52.201.10.13.

ويتضح أيضا أن كلًّا من (اسم الشركة، وعنوان البريد الإلكتروني، وعنوان بروتوكول الإنترنت) مرتبط بروابط خارجية، وهو ما يساعد على التوصل إلى أسماء نطاقات أخرى مرتبطة بشركة Newsweek ذات المسؤولية المحدودة، مثل ibtimes.com وغيره من المواقع المستضافة على نفس عنوان بروتوكول الإنترنت. ولمثل هذه الروابط والاستنتاجات أهمية خاصة في عملية التحقق، ولا يمكن الاستغناء عن النظر في المواقع الأخرى المسجلة باسم شخص أو شركة ما.

وفيما يتعلق بعناوين بروتوكول الإنترنت، فلا بدّ من التنبه إلى أنه من الممكن أن تتمّ استضافة مواقع إلكترونية على نفس الخادم، لكن هذا لا

يعني بالضرورة أن بينها علاقة ما أو أنها ضمن شبكة واحدة. فذلك يحدث عادة لأن أصحاب هذه المواقع قد يستفيدون من خدمات شركة واحدة لاستضافة مواقعهم الإلكترونية على الويب.

لكن يمكن -كقاعدة عامّة- أن نشير إلى أنه كلما كانت المواقع المشتركة على خادم واحد أقل عددًا، فإن هذا يزيد من احتمال كونها مرتبطة فيما بينها، ولكن يبقى ذلك أمرًا يحتاج إلى التحقق والتأكّد.

فلو رأيت أن أحد الخوادم يستضيف مئات المواقع، فقد لا تكون هنالك على الأغلب علاقة بينها. لكن لو تحريت عن موقع ما، ووجدت أنه مرفوع على خادم يستضيف ثمانية مواقع أخرى مثلًا، فهذا يعني ضرورةَ التحقق من هذه المواقع الثمانية، والبحث عنها عبر أداة whois؛ لتتأكد إن كانت مسجلة باسم نفس الشخص أو الشركة التي تملك الموقع الذي تتحرى عنه.

كما تجدر بنا الإشارة إلى أن بعض الجهات قد تدفع لحماية خصوصية بيانات التسجيل الخاصة بأحد مواقعها، ولكنها قد تهمل ذلك في مواقعها الأخرى.

إن ملاحظة هذه العلاقات بين المواقع عبر استخدام عنوان بروتوكول الإنترنت، وبيانات تسجيل الموقع و/أو المحتوى يعد وسيلة أساسية للكشف عن وجود شبكة وراءها وتحديد الأطراف المسؤولة عنها. وسنستعرض الآن طريقة أخرى للبحث عن العلاقات بين المواقع الإلكترونية، وذلك عبر استخدام الكود الخاص بصفحة الويب.

تحليل كود الموقع الإلكتروني

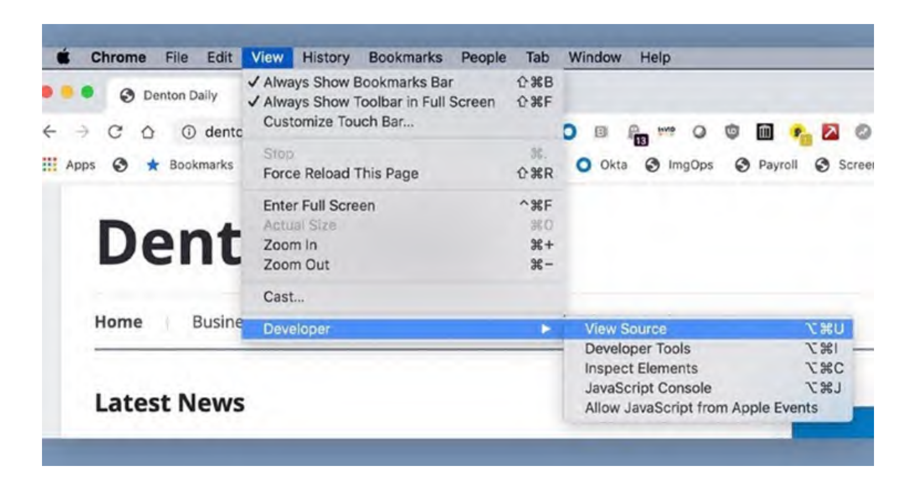
هذه الطريقة التي يعود الفضل في اكتشافها إلى لورنس ألكساندر تعتمد على عرض الكود المصدر لصفحة الويب ثم استخدامه في البحث في محاولة للكشف عن كود خاصة بجوجل أناليتيكس و/أو جوجل أدسينس، وهما أداتان معروفتان من جوجل، تُقدِّم الأولى لصاحب الموقع

الإحصائيات والأرقام التي تساعده عمومًا في معرفة أداء الموقع ومحتواه، أما الثانية فتساعده على كسب المال عبر الإعلانات.

وبمجرد ربط الموقع الإلكتروني بهاتين الأداتين أو إحداهما، فسيكون لكل صفحة ويب رقم تعريف مرتبط بحساب صاحب الموقع على جوجل أناليتيكس أو آدسينس. وفي حال كان هنالك أكثر من موقع إلكتروني يتبع لنفس الشخص أو الجهة، فإنه عادة ما يقوم بربط جميع المواقع التابعة له بحساب واحد على جوجل أنالتيكس وآدسينس للتمكن من مراقبتها والتحكم بها.

وتشكّل هذه الحالة فرصة للصحفي الذي يتحرّى عن موقع أو مجموعة من المواقع تساعده على إيجاد الرابط بينها عبر اكتشاف رقم التعريف (ID) المشترك بحساب جوجل أناليتيكس أو آدسينس في كود المصدر الخاص بالموقع. ولحسن الحظ فإن الكشف عن ذلك ليس عملية صعبة.

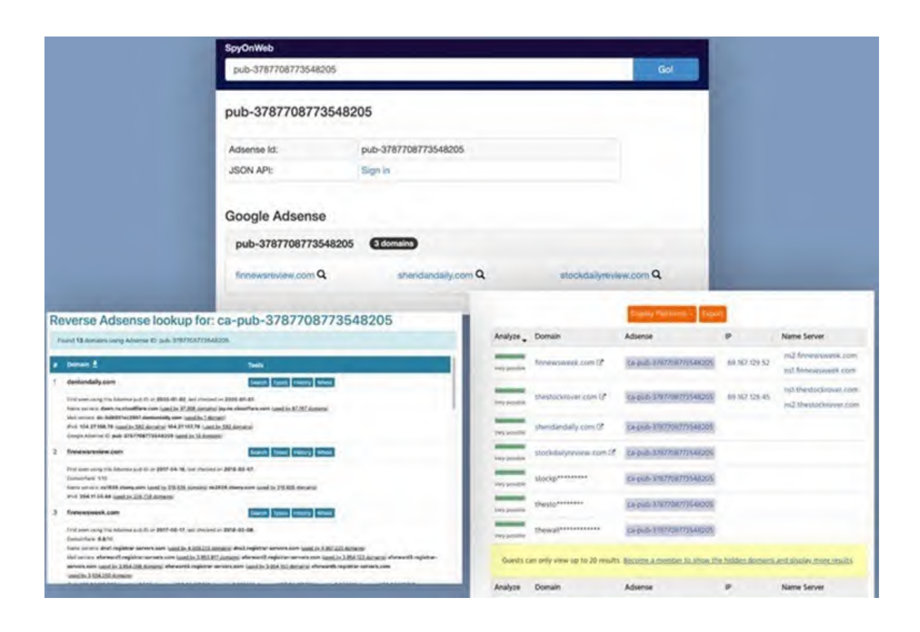
اذهب إلى الموقع الذي تقوم بالتحري عنه، ولنستخدم هنا على سبيل المثال موقع dentondaily.com؛ فإنْ كنت في متصفح جوجل كروم على جهاز آبل ماك، فانقر على قائمة العرض "View"، ثم اختر "Developer"، ثم عرض المصدر "View Source". وستظهر لديك نافذة تبويب جديدة يظهر عليها الكود المصدر. أما لو كنت تستخدم جهاز حاسوب بنظام ويندوز فيمكنك بسهولة الوصول إلى الكود المصدر عبر الضغط على (Ctrl+U).



جميع أرقام تعريف التتبع (ID) الخاصة بجوجل أناليتيكس تبدأ بالحرفين "ua"، يليهما رقم من عدة خانات. أما أرقام التعريف الخاصة بآدسينس فتبدأ بالرمز "pub" يتبعه رقم من عدة خانات. لذا فإنه من السهل العثور على رقم التعريف الخاص بالأداتين عبر عملية بحث بسيطة في الكود المصدر، عبر الضغط على Command-F في أجهزة ماك أو Ctrl-F على الأجهزة الأخرى، ثم كتابة الرمز -ua أو -pub ليظهر لك رقم التعريف على الصفحة.

```
view-source:https://dentondaily.com
Apps   Bookmarks   pub-   2/3
75
76
77                  <script async src="https://pagead2.googlesyndic
78 <!-- Top Responsive -->
79 <ins class="adsbygoogle"
80      style="display:block"
81      data-ad-client="ca-pub-3787708773548205"
82      data-ad-slot="3224711756"
83      data-ad-format="auto"
84      data-full-width-responsive="true"></ins>
85 <script>
86      (adsbygoogle = window.adsbygoogle || []).push({});
87 </script>
88                </div><!-- /.adv --> <div class="clear"></div>
89
```

عند العثور على رقم التعريف الخاص بهاتين الأداتين أو إحداهما، قم بنسخه والبحث عنه في صندوق البحث على أدوات مثل SpyOnWeb أو DNSlytics أو NerdyData أو AnalyzeID. تنبه إلى أنك قد تحصل على نتائج مختلفة بحسب الأداة التي تستخدمها، لذا فإنه من الضروري أن تقارن النتائج في أكثر من أداة لتتحقق بشكل جيد من النتيجة. لاحظ مثلًا في الصورة أدناه كيف أن أداة SpyOnWeb قد حددت 3 أسماء نطاق تستخدم نفس رقم التعريف الخاص بآدسينس، بينما أظهرت أداة DNSlytics وأداة AnalyzeID نتائج أكثر.



مـن الضــروري التنبــه كذلــك إلــى أن موقعًــا مــا قــد يكــون اســتخدم رقــم التعريــف بــأداة جوجــل أناليتيكــس أو آدســينس فــي وقــت ســابق، لكــنّ الموقــع لــم يعــد موجــودًا، وهــذا يعنــي أنــه مــن الضــروري اســتخدام نفــس الطريقــة الخاصــة بالبحــث عبــر الكــود المصــدر فــي أي مواقــع أخــرى تشــير الأدوات التــي اســتعنت بهــا إلــى أنهــا تســتخدم رقــم تعريــف واحــد لأنالتيكــس أو آدســينس للتأكد من أنها موجودة.

لاحــظ أيضًــا أن أرقــام التعريــف الخاصــة بأناليتيكــس وآدســينس مــا تــزال موجــودة فــي النســخة المؤرشــفة مــن الموقــع علــى Wayback Machine. ففــي حــال لــم تجــد رقــم التعريــف علــى موقــع فعــال؛ فــلا تنــس أن تبحــث عنــه أيضًا عبر أداة Wayback Machine.

جميــع هــذه الأدوات تقــدِّم بعــض الخدمــات المجانيــة التــي تســاعد فــي الحصــول علــى بعــض النتائــج، ولكــن عــادة مــا يضطــر الصحفــي إلــى اســتخدام النســخة المدفوعــة مــن بعــض الأدوات للحصــول علــى النتائــج الكاملــة، خاصــة إن كان رقــم التعريــف الــذي تبحــث عنــه مســتخدَمًا فــي عــدد كبيــر مــن المواقــع الأخرى.

الملاحظـة الأخيـرة فيمـا يتعلـق بالبحـث فـي الكـود المصـدر هـو أنـه قد يكـون مـن المفيـد النظـر سـريعًا فـي صفحـة الكـود، حتـى لـو لـم تكـن تفهـم لغـات البرمجــة مثـل HTML أو جافاسـكريبت أو PHP أو غيرهـا مـن اللغـات المعروفـة؛ فقـد يحصـل أحيانًـا أن ينسـى المبرمِـج تغييـر عنـوان صفحـة أو موقـع إن كان يسـتخدم نفس قالـب التصميـم لعـدة مواقـع، وقـد يسـاعد التصفّـح السـريع للكـود المصـدر علـى الكشـف عـن مثـل هـذه الأخطـاء التـي تسـاعد في الكشف عن علاقةٍ ما بين عدّة مواقع.

وقـد حصـل أثنـاء عمليـة التحقـق التـي أجريتهـا بخصـوص عمليـة الاحتيـال الخاصــة بالإعلانــات والتــي اسـتعانت بمواقـع لشـركات وهميّـة مثـل Ato-ses أننـي كنـت مهتمًّـا بمتابعـة شـركة تدعـى FLY Apps. وقـد تصفحـتُ الكـود المصـدر لموقـع الشـركة الإلكترونـي والـذي كان يتضمـن صفحـة ويـب وحيـدة، ولاحظـت فـي بدايـة الكـود كلمـة "Loocrum" كمـا يظهـر فـي الصورة أدناه.

```
317 <input type="submit" name="submit" value="" style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-
    box-sizing: border-box; color:inherit;font:inherit;font-family:inherit;font-size:inherit;line-
    height:inherit;-webkit-appearance:button;cursor:pointer;background-
    image:url('https://archive.is/lG6hf/de442e0343d248b28ace0397c40e6769735eeaf8.svg');background-color:
    transparent; width:18px;height:14px;text-indent:-9999px;background-repeat: no-repeat; border-width: medium;
    border-style: none; margin: 0px; border-color: white; "/>
318 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
    </div>
319 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
    </form>
320 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
    </div>
321 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    display:table;clear:both;"> </span></div>
322 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    display:table;clear:both;"> </span></div>
323 <div style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    background-color: rgb(141, 118, 190); position:absolute;top:0px;right:0px;bottom:0px;left:0px;z-
    index:5;display:none;"><span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing:
    border-box; "></span>
324 <div style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    margin-right:auto;margin-left:auto;padding-left:15px;padding-right:15px;"><span style="box-sizing: border-
    box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; display:table;"> </span>
325 <span style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-
    box; float:left;line-height:20px;font-family:ralewayblack, sans-serif;font-size:29px;text-
    transform:uppercase;height:auto;margin-left:15px;margin-top:9px;color:rgb(255, 255, 255);padding: 3px 15px;
    "><span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; ">
    </span>Loocrum<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    "></span></span>
326 <div style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    float:right;margin: 24px 5px 0px 0px; "><span style="box-sizing: border-box; -moz-box-sizing: border-box; -
    ms-box-sizing: border-box; "></span>
```

فبحثـت فـي جوجـل عـن هـذه الكلمـة ووجـدت أنهـا تعـود لشـركة تدعـى Loocrum، والتـي تسـتخدم تصميمًـا مماثـلًا تمامًـا لموقـع FLY Apps،

إضافة إلى التشابه بينهما في جزء من المحتوى. وقد كشف البحث عبر Whois أن عنوان البريد الإلكتروني المستخدم في تسجيل موقع Loocrum.com هو نفسه الذي استخدم في تسجيل مواقع الشركات الوهمية الأخرى التي كنت أتحرى عنها، وقد كان ذلك دليلًا إضافيًّا على أن الأشخاص الأربعة المسؤولين عن FLY Apps كانوا أيضًا متورطين في عملية الاحتيال، وقد تمكنت من التوصل إلى ذلك عبر عملية تصفّح بسيطة للكود المصدر؛ بحثًا عن بعض الكلمات اللافتة التي قد تفيد في عملية البحث.

خاتمة

جميع هذه العمليات والأدوات -رغم فائدتها- قد لا تكون كافية للتوصّل إلى النتيجة التي تبحث عنها، وقد تشعر في النهاية بأنك قد وصلت إلى طريق مسدود. لكن هذا -في المقابل- لا يعني الاستسلام؛ إذ يمكن التوصل إلى أدلّة جديدة تفيد في التحقيق الذي تقوم به عبر متابعة دراسة الروابط الموجودة على المواقع الإلكترونية موضوع التحقيق، أو فحص المحتوى، وقراءة الشيفرات المصدرية للمواقع، وتتبع الأشخاص الذين ينشرون محتواها أو يُوصون به وملاحظة أي تفاصيل أخرى قد تساعد في الكشف عن حقيقة ما يجري.

الفصل التاسع: تحليل الإعلانات على شبكات التواصل الاجتماعي

جوهانا وايلد

جوهانا وايلد: محققة مختصة بالمصادر المفتوحة في مؤسسة Bellingcat، ويتركز اهتمامها على الجوانب التقنية وتطوير الأدوات للاستخدام في التحقيقات الصحفية الرقمية، ولديها خبرة في مجال صحافة الإنترنت. عملت سابقًا مع صحفيين في مناطق صراع أو مناطق شهدت صراعات سابقة، وهي ناشطة في دعم الصحفيين في شرق أفريقيا لإنتاج مواد ونشرها مع إذاعة "صوت أمريكا".

إن الإعلانات التي تراها وأنت تتصفح منصات التواصل الاجتماعي ليست هي نفسها التي يراها زميلك الذي يجلس بجانبك أثناء تصفحه نفس تلك المنصات. فثمّة معطيات تحدّد نوع الإعلانات التي تظهر لدى كل شخص، مثل الموقع أو الجنس أو العمر أو حتى الإعجابات التي تضعها على المنشورات التي تراها أو الروابط التي شاركتها وغير ذلك من العوامل. فقد يظهر لديك إعلانات لفنادق فخمة في أنطاليا أما زميلك فقد تظهر له إعلانات تتعلق بتطبيقات ألعاب يابانية.

هذه العمليات من الاستهداف الدقيق (Microtargeting)، تعمل على تصنيف مستخدمي منصات التواصل الاجتماعي إلى مجموعات مستهدَفة؛ بحيث يظهر لكل منها إعلانات تناسب ظروفهم واهتماماتهم، وهي عمليات تثير الكثير من الجدل؛ خاصة في سياق الانتخابات.

فثمة قلقٌ لدى المعنيين بأن الحملات الانتخابية قد تستهدف فئات صغيرة معينة من السكان عبر إعلانات تبث الخوف أو تنشر الكراهية أو تروج

لمعلومات زائفة.

ويزيد من خطورة هذا الأمر أن الإعلانات التي تنشرها الحملات الانتخابية على شبكات التواصل الاجتماعي لا تخضع لعمليات التحقق من المعلومات من قبل المنصات نفسها. فشركة فيسبوك أكدت في يناير 2020 أنها لن تمنع أي إعلان سياسي إن كان ملتزمًا بـ "معايير المجتمع" الخاصة بالمنصة، وهذا يعني إتاحة المجال لاستهداف مجموعات محددة من المستخدمين بإعلانات قد تشتمل على معلومات مضللة حول قضايا سياسية واجتماعية حساسة.

وحتى فترة قريبة، كان من شبه المستحيل على الصحفيين والباحثين أن يتوصلوا إلى معلومات تتعلق بالإعلانات الموجَّهة إلى مجموعات مختلفة من المستخدمين، ولم يتحقق لهم ذلك إلا بعد أن تصاعدت الانتقادات ضد منصات التواصل الاجتماعي حول غياب الشفافية في هذا الجانب، ما اضطر العديد منها إلى إنشاء سجلات خاصة بالإعلانات تتيح للجميع مراجعة المعلومات الخاصة بالإعلانات التي نشرت على المنصة.

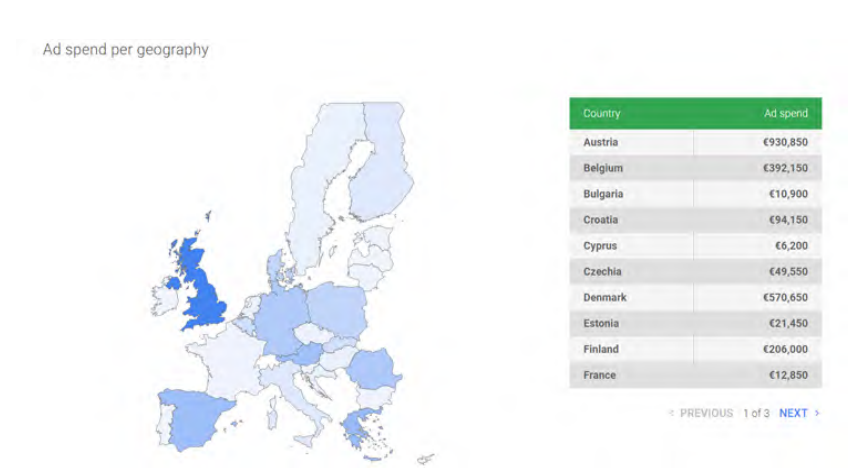
ومع ذلك فإن "مكتبة الإعلانات" في فيسبوك ما تزال تواجه العديد من الانتقادات التي تتهم الشركة بعدم تقديم معلومات موثوق بها بشكل كاف بخصوص كافة الإعلانات التي يتم نشرها على المنصة.

وقد يلزمك التحقق أحيانًا أثناء استخدام مكتبة الإعلانات في فيسبوك من أن كافة الإعلانات التي تظهر لديك أثناء تصفح المنصة تظهر بالفعل في المكتبة.

لكن تعتبر مكتبات الإعلانات خطوة مهمّة لتعزيز الالتزام بالشفافية وتسهيل مهمة الصحفيين والمراقبين في عمليات التحقق من الإعلانات الرقمية ونشاطها. وستكون قادرًا عبر دراسة الأساليب التي سنستعرضها فيما يلي على اكتساب المهارات الأساسية للتحقق من الإعلانات على المنصات الرقمية الأكبر مثل جوجل وتويتر وفيسبوك.

جوجل

يشكّل القسم الخاص بالإعلانات في جوجل جزءا مهمًا في كواليس تقرير الشفافية الذي تقدّمه الشركة. ويمكن عبر هذا الرابط الوصول إلى القسم الخاص بالإعلانات السياسية، والذي يقدم معلومات عن إعلانات جوجل ويوتيوب من الاتحاد الأوروبي والهند والولايات المتحدة الأمريكية، حيث يظهر في الصفحة الخاصة بكل منطقة قائمة بالدول ومجموع من أنفق على الإعلانات منذ إطلاق التقرير.



Country	Ad spend
Austria	€930,850
Belgium	€392,150
Bulgaria	€10,900
Croatia	€94,150
Cyprus	€6,200
Czechia	€49,550
Denmark	€570,650
Estonia	€21,450
Finland	€206,000
France	€12,850

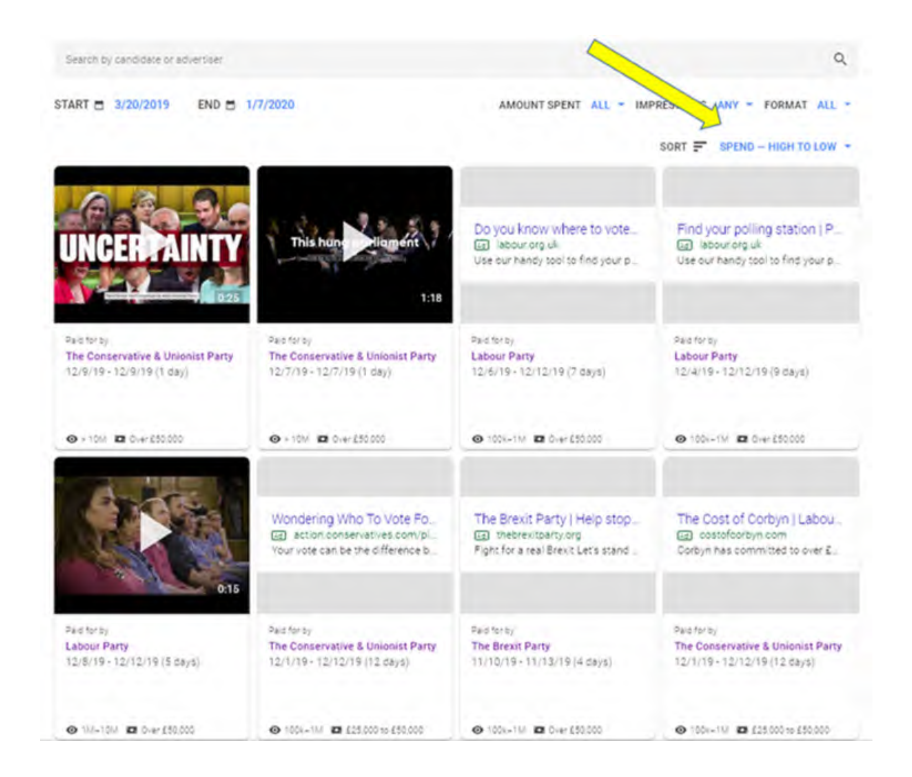
وعبر الضغط على اسم الدولة ستصل إلى الصفحة التي تشتمل على قاعدة البيانات الخاصة بالإعلانات:



ويمكنك عرض النتائج حسب التاريخ، أو المبلغ الذي تم إنفاقه، أو عدد مرات ظهور الإعلان للمستخدمين (Impressions). كما يمكن عرض النتائج حسب شكل الإعلان، سواء كان فيديو أم صورة أم نصًّا.

يساعد هذا التقرير على معرفة الجهات الأكثر إنفاقًا على الإعلانات. فلو

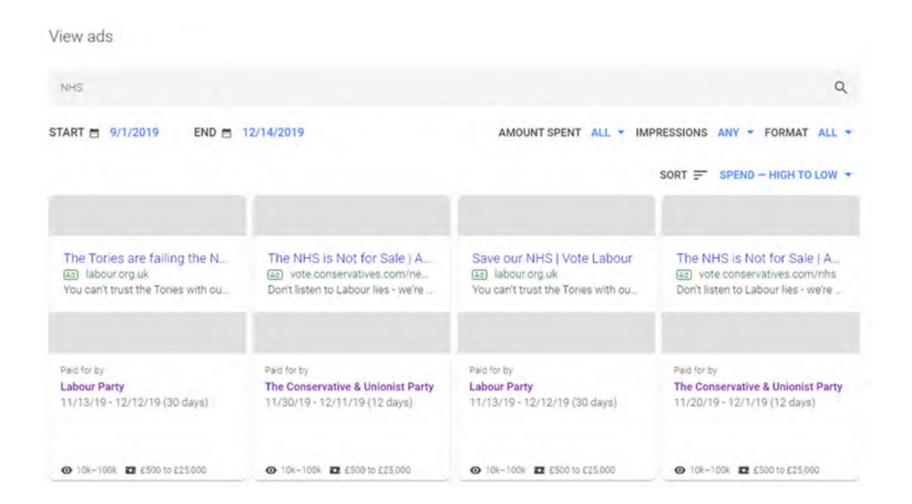
أردت مثـلًا اسـتعراض أكبـر الحمـلات الإعلانيـة السياسـية فـي المملكـة المتحـدة منـذ انطـلاق التقريـر حتـى ينايـر 2020، فمـا عليـك سـوى ترتيـب عـرض النتائـج حسـب الإنفـاق مـن الأعلـى إلـى الأقل (SPEND-HIGH TO LOW)، كما يظهر في الصورة أدناه:



وكمـا هـو متوقّـع، فـإن الإنفـاق كان أكثـر فـي يـوم الانتخابـات العامـة واليـوم الـذي سـبقه، وكان ذلـك فـي 12 ديسـمبر 2019. سـتلاحظ كذلـك أن حـزب المحافظيـن قـد أنفـق أكثـر مـن 50 ألـف جنيـه إسـترليني علـى إعلانيـن علـى يوتيـوب لمـدة يـوم واحـد فقـط. أمـا حـزب العمـال فـي المقابـل فقـد صـرف أكثـر مـن 50 ألـف جنيـه إسـترليني علـى إعـلان علـى صفحـات البحـث فـي جوجـل لأداة قـال الحـزب إنهـا ستسـاعد المواطنيـن علـى العثـور علـى مراكـز التصويت بسهولة.

Find your polling station | Plan your journey
Ad labour.org.uk
Use our handy tool to find your polling station Make sure you know where to vote on Thursday 12 December.

يمكن البحث كذلك عبر كلمة مفتاحية. فلو كتبت NHS (هيئة الخدمات الصحية الوطنية في بريطانيا)، فستجد أن حزب العمال وحزب المحافظين قد دفعوا لصالح إعلانات في محرك البحث جوجل خلال نوفمبر وديسمبر 2019 للترويج لمحتوى ينتقد فيها كل حزب خطط الآخر فيما يتعلق بالهيئة.



وعند النقر على اسم الجهة المعلنة سيكون بوسعك معرفة مجموع المبلغ الذي أنفقَتْه على إعلانات جوجل منذ أول تقرير تم إطلاقه. وقد كان حجم إنفاق الحزبين الرئيسيين في المملكة المتحدة حتى يناير 2020 على النحو التالي:

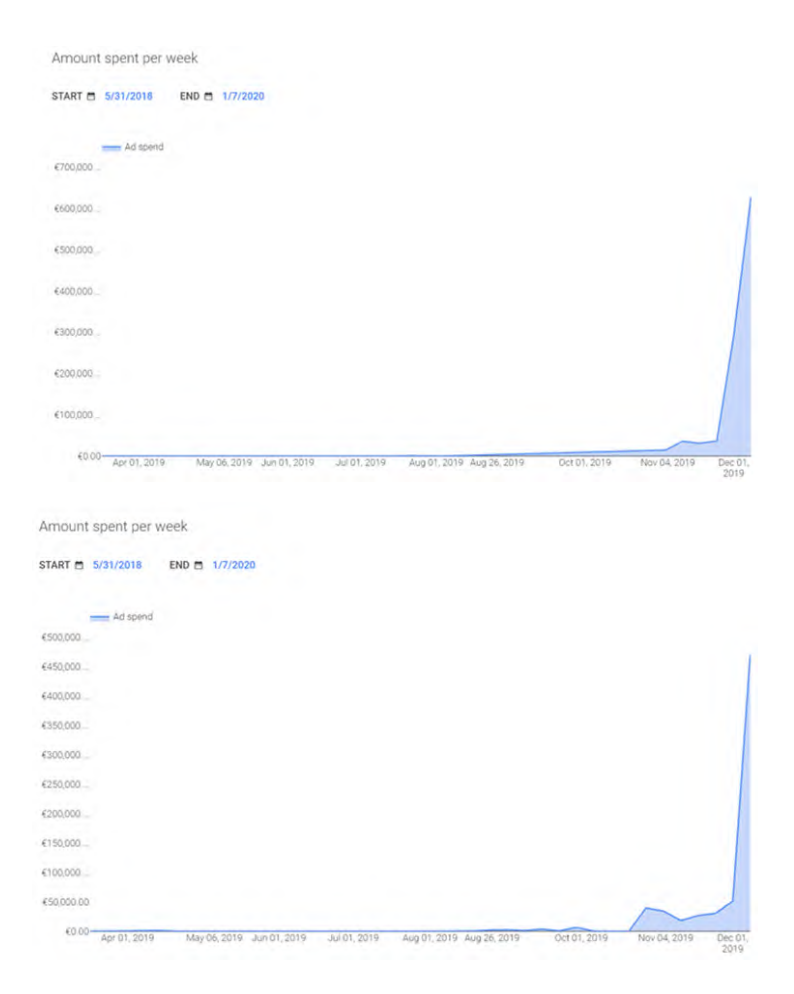


Advertiser: Labour Party

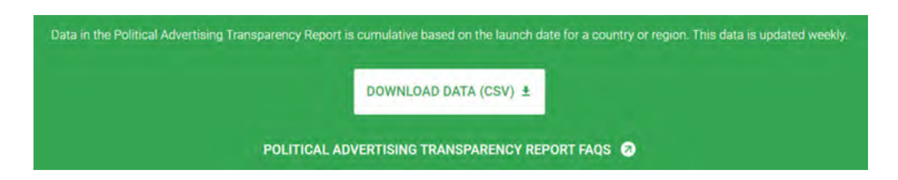
Ads
94

Amount spent
€693,200
£587,350.00

يمكن كذلك عرض خط زمنيّ لهذا الإنفاق، فالتقارير أدناه تظهر أنماط الإنفاق لدى الأحزاب، الأول لحزب المحافظين والثاني لحزب العمال:



وإن كنت ترغب بالتعمق في قاعدة البيانات الخاصة بالإعلانات وتحليلها بشكل أوسع، فيمكن أن تستمر بتصفح التقرير إلى الأسفل حتى تصل إلى شريط باللون الأخضر يتيح لك تنزيل البيانات في ملف بصيغة CSV.

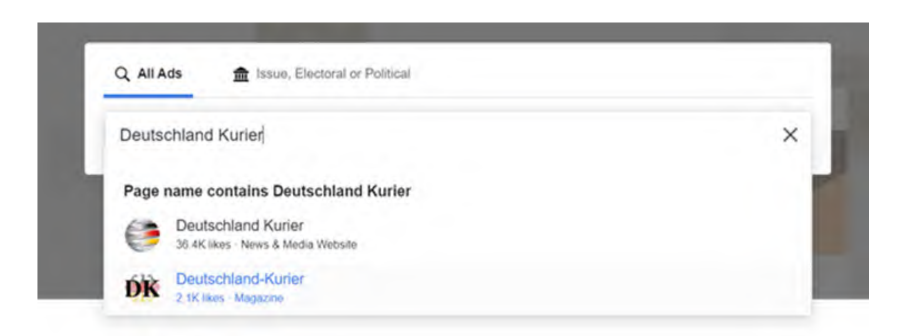


يمكنك بعدها نقل البيانات وعرضها على برنامج جداول؛ مثل إكسل، أو جداول بيانات جوجل، وذلك للقيام بالمزيد من عمليات التحليل والفلترة.

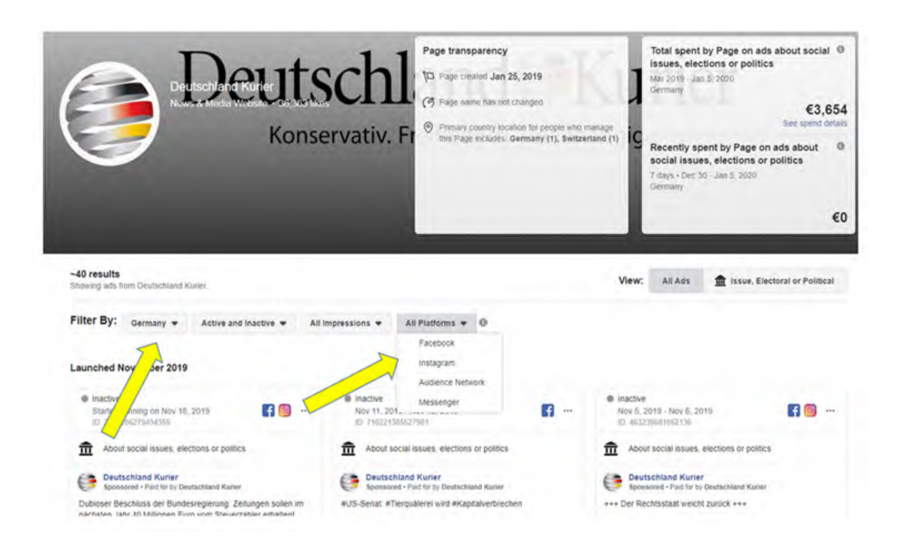
فيسبوك

تنقسم مكتبة الإعلانات في فيسبوك إلى قسمين: "جميع الإعلانات" (All Ads) أو "الموضوع، الانتخابات، السياسة" (Issue, Electoral or Political). لو اخترت "جميع الإعلانات" فستتمكن من البحث عن معلِنين محدَّدِين باستخدام الاسم فقط، وليس باستخدام الكلمات المفتاحية.

فلو أردنا مثلًا البحث عن إعلانات من مجلة Deutschland Kurier، والتي عادة ما تنشر محتوى مؤيدًا لحزب "البديل من أجل ألمانيا" اليميني المتطرف، فيمكن البحث عبر الاسم، وستظهر اقتراحات بأسماء الصفحات القريبة منه.



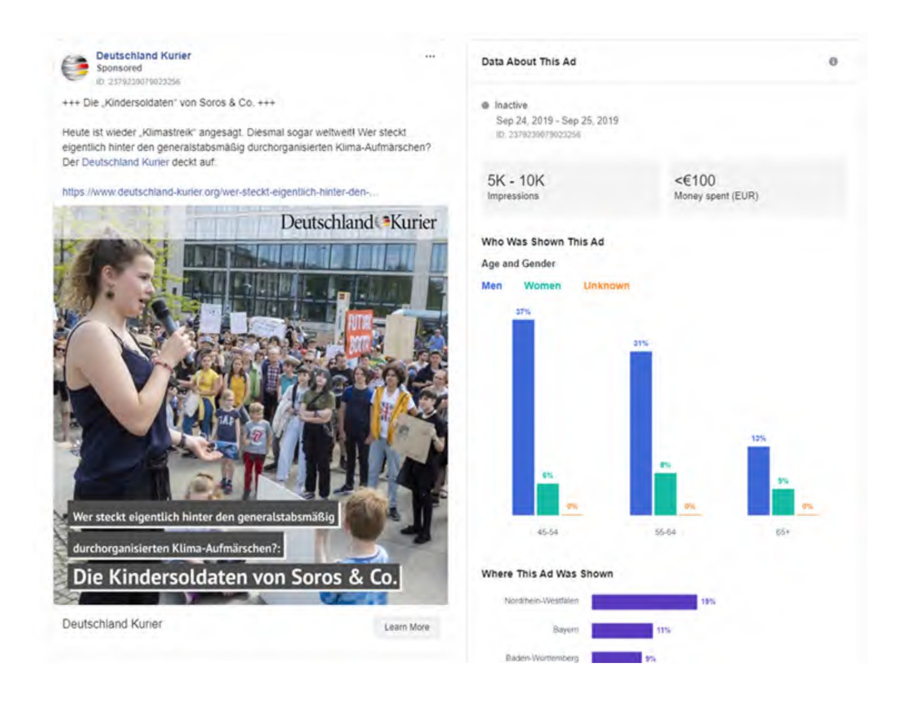
وتظهر صفحة النتائج أن هذه المجلة أنفقت 3,654 يورو على الإعلانات في ألمانيا بين مارس 2019 ويناير 2020.



تأكد حين تصل إلى صفحة النتائج من عرض النتائج حسب الدولة إن كنت معنيًّا بذلك، أو جميع الدول، وأن تحدد ما إذا كنت تريد عرض الإعلانات من فيسبوك أو إنستغرام أو ماسنجر أو شبكة الجمهور من فيسبوك (Facebook Audience Network)، وهي شبكة لتشغيل إعلانات على تطبيقات الموبايل والمواقع الإلكترونية الأخرى.

الخيار الأسلم في معظم الحالات هو البحث عن الإعلانات في جميع المنصات من أجل الحصول على صورة واضحة لنشاط الإعلان الذي تتبعه المؤسسة أو الجهة التي تبحث عنها.

ويمكن عرض التفاصيل الخاصة بكل إعلان على حدة، عبر النقر على خيار "See ad details" لاستعراض المزيد من المعلومات.



يظهر في هذا المثال أن هذه المجلة قد أنفقت ما يقارب 100 يورو على هذا الإعلان الذي يصف المتظاهرين المدافعين عن البيئة بأنهم "مجنّدون أطفال لصالح سوروس وشركاه". وحصد الإعلان بين 5 آلاف إلى 10 آلاف ظهور، وعرض بشكل أساسي من قبل مستخدمين ذكور بالفئة العمرية 45 عامًا وأكثر.

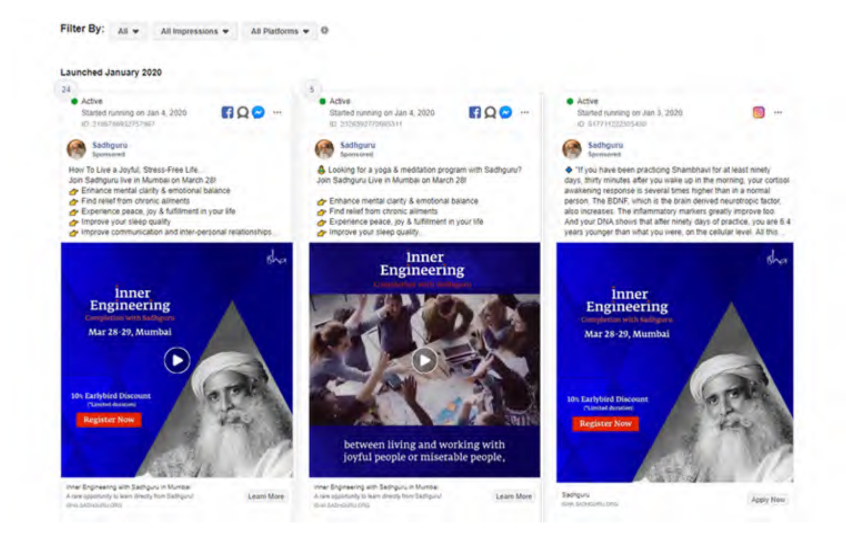
أما الخيار الثاني فهو البحث في مكتبة الإعلانات حسب الموضوع (قضايا اجتماعية) أو الإعلانات المتعلقة بالانتخابات، أو المتعلقة بالقضايا السياسية. والميزة الكبرى في هذا الخيار هي إمكانية البحث عبر أي كلمة مفتاحية ترغب بها في الإعلانات التي يؤرشفها فيسبوك.

ولننظر معًا إلى هذا المثال. سادجورو (Sadhguru) هو شخصية هندية معروفة في عالم الروحانيات والتصوف، وهو ليس محسوبًا على أي حزب سياسي، وهو القائل أن من واجبه دعم أي حكومة كانت من أجل "تقديم أفضل ما لديها". لو كتبت اسمه في قسم "جميع الإعلانات"

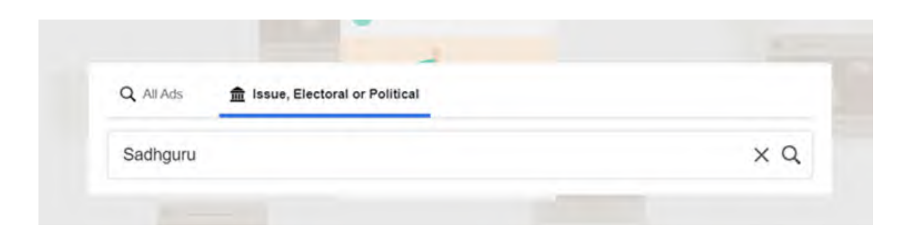
فـي مكتبـة الإعلانـات فـي فيسـبوك، فسـتظهر لك الصفحة الرسـمية الشـخصية لهذا الرجل.



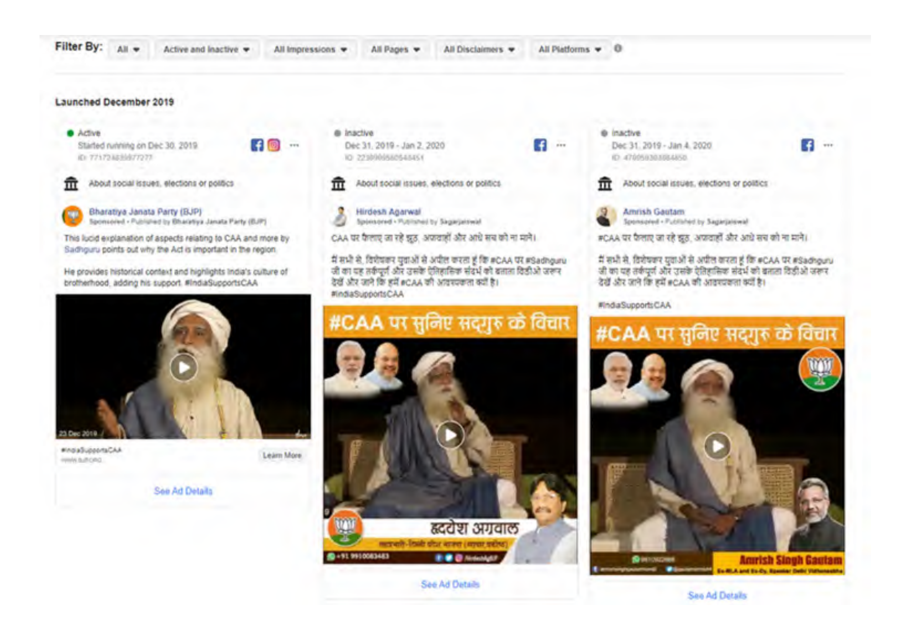
كمـا سـتجد عـددًا مـن الإعلانـات غيـر السياسـية التـي نشـرتها الصفحة والتـي يروّج فيها لبرامجه التدريبية في مجال اليوغا والتأمل.



أمـا الآن فسـنبحث عـن اسـمه فـي قسـم "-Issue, Electoral or Politi cal" في المكتبة دون اختيار الصفحة الرسمية الخاصة بالرجل:



وستجد أن النتائج اختلفت بشكل كبير، حيث سنعثر على الإعلانات التي ذكرت اسم سادجورو، والتي نشرتها حسابات أخرى لا علاقة لها بالصفحة الرئيسية للرجل:



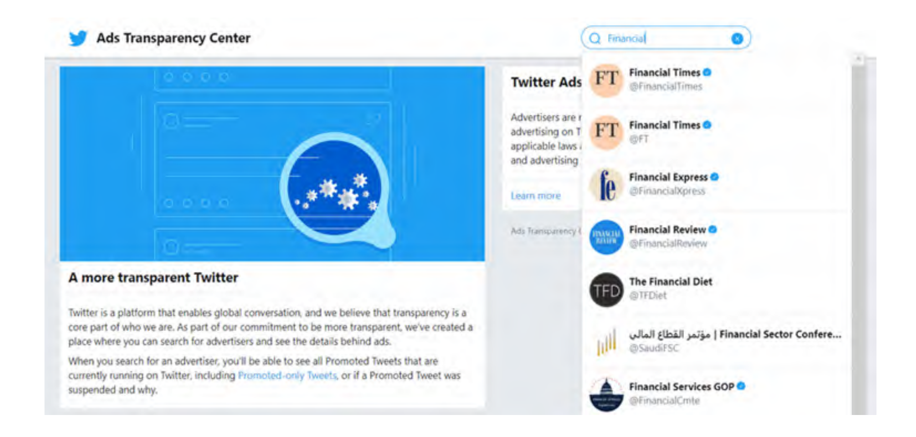
أحد الإعلانات من حزب بهاراتيا جاناتا الحاكم في الهند يَظهر فيه مقطع فيديو يعلن فيه سادجورو عن دعمه لتعديل قانون الجنسية المثير للجدل في الهند، والذي يتيح لبعض المهاجرين غير المسجَّلين من بعض الدول المجاورة للهند الحصول على الجنسية الهندية باستثناء المسلمين. ويتضمن الإعلان إشارة محتملة إلى العلاقة المحتملة بين سادجورو والحزب الحاكم، وهو موضوع ما يزال يثير الكثير من النقاش والجدل في الهند.

يُظهر هذا المقال كيفية استخدام مكتبة الإعلانات من فيسبوك للبحث عن المزيد من المعلومات عبر بعض الكلمات المفتاحية المتعلقة بموضوع التحقيق.

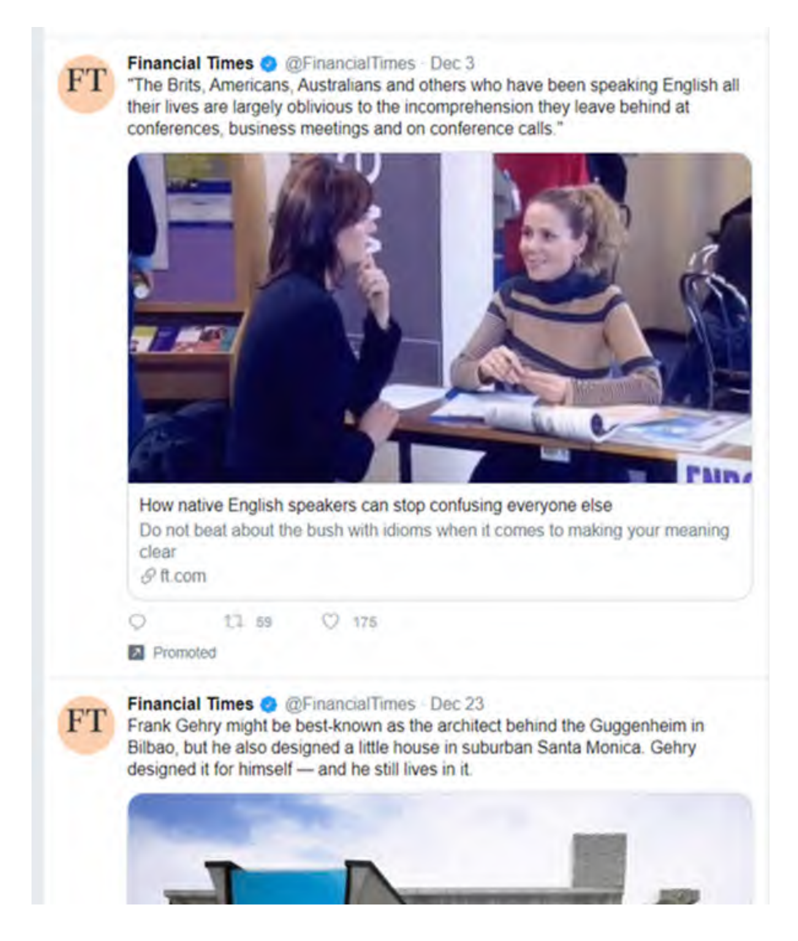
وقد يلزمك كذلك الاطلاع على تقرير مكتبة الإعلانات في فيسبوك، والذي يقدّم بعض المعلومات الإجمالية الأساسية بخصوص الإعلانات السياسية في دول مختلفة.

تويتر

في نهاية العام 2019 قررت تويتر حظر الإعلانات المرتبطة بأغراض سياسية على منصتها. ومع ذلك، يمكنك الرجوع إلى مركز شفافية الإعلانات في تويتر للتحري عن الإعلانات غير السياسية المنشورة خلال سبعة أيام سابقة. لكن يصعب العثور على إعلان محدد، وذلك بسبب عدم توفر ميزة البحث عن الكلمة المفتاحية. للبدء بعملية البحث، اذهب إلى صندوق البحث في الزاوية العليا اليمنى واكتب اسم المستخدم الذي تود البحث عن إعلاناته:



وفـي حـال كان الحسـاب قـد نشَـر أيـة إعلانـات خـلال الأيـام السـبعة الماضيـة فسيكون بوسعك الاطلاع عليها.



يمكـن أن نلاحـظ أن الفايننشـال تايمـز قـد دفعـت لإعـلانٍ علـى تويتـر؛ رغبـة فـي الترويـج لمقـال عـن اللغـة الإنجليزيـة. كانـت التغريـدة قـد نشـرت فـي 3 ديسـمبر 2019، ولكـن المعلومـات الخاصـة بالإعـلان لا تذكـر متـى تـم تفعيل الإعلان بالضبط.

ولتسـريع عمليـة البحـث يمكـن اسـتخدام حيلـة بسـيطةٍ عنـد بـدء عمليـة البحث، انظر إلى الرابط على المتصفح الذي تستخدمه:

ads.twitter.com/transparency/FinancialTimes

يمكن -عبر تعديل الجزء الأخير فقط- أن تبحث عن حساب آخر، دون الاضطرار للذهاب إلى مركز الإعلانات والبدء بعملية البحث من جديد. فقط اكتب اسم المستخدم في النهاية، وستحصل على قائمة الإعلانات التي نشرها.

ads.twitter.com/transparency/Bellingcat

وفي حال لم تكن هنالك إعلانات من الحساب خلال الأيام السبعة الماضية، فستحصل على رسالة تفيد بأنه هذا الحساب لم يدفع لأي إعلانات جديدة في الأيام السبعة الماضية. وبما أن مركز شفافية الإعلانات في تويتر لا يتيح سوى الاطلاع على الإعلانات المنشورة خلال سبعة أيام، فسيكون من اللازم التحقق بشكل دوري على نشاط الإعلانات للحساب الذي تودّ تحليل نشاطه، ولا تنس لقطات الشاشة "Screenshots" في حال وجدت أي إعلان من طرفه.

سناب شات

تقدم مكتبة الإعلانات السياسية في سناب شات معلومات تتعلق بالإعلانات السياسية أو المرتبطة ببعض القضايا الاجتماعية أو حملات المناصرة، وهذا يشمل بحسب تعريف المنصة الإعلانات المتعلقة بالقضايا أو المنظمات التي تكون موضوع نقاش عام على المستويات المحلية أو الوطنية أو العالمية، أو ذات الأهمية الخاصة للعامة، مثل القضايا المتعلقة بالتعليم أو الهجرة أو حيازة الأسلحة.

ستجد في مكتبة الإعلانات قائمة بالسنوات:

Archives

2018

2019

2020

اضغط على أحد هذه الأعوام لتنزيل جدول بيانات يشتمل على كافة المعلومات المتعلقة بإعلانات ذلك العام. سيلزمك القليل من الصبر في البداية للتعامل مع هذه الجداول التي قد تبدو للوهلة الأولى ليست مرتبة، ولكنها في الواقع كذلك. فكل سطر يخصُّ إعلانًا محدّدًا، ويوضح فيه من نشر الإعلان، وكم صرف عليه، إضافة إلى توضيح المستخدمين المستهدفين به.

16 3e4c8332c 2,64E+08 I
17 a5b7f6d8c362e1810d41be049569f0a76fb80a6020411bfa5e5f0a4744df484c,https://www.snap.com/political-
18 ads/asset/a0ee86600cda141a006c4a4c60c5d4dd9c78f23dbf08a3ac9329b51fa5d76fe6?mediaType=mp4,EUR,315,417284,2020/01/06 05:30:55Z,2020/01/11 22:30:55Z,Ja zum Schutz,CH,Ja zum Schutz,Ja
19 zum Schutz,,18+,switzerland,,"Fribourg,Geneve,Jura,Neuchatel,Ticino,Valais,Vaud",,,,,,,,,,,"Adventure Seekers,Arts & Culture Mavens,Beachgoers & Surfers,Beauty Mavens,Bookworms & Avid
20 Readers,Collegiates,Foodies,Hipsters & Trendsetters,Political News Watchers,Outdoor & Nature Enthusiasts,Pet & Animal Lovers,Philanthropists,Worldly Travelers,Women's Lifestyle",,Provided by
21 Advertiser,"de,en",,,,web_view_url:https://jazumschutz.ch/fahne-snap
22 cfb4d1da728d946f5fbcec8b9e409f76150ba9e1a6764228e42eb76082b7b5f8,https://www.snap.com/political-ads/asset/6fcf8e70b0690c182e8b3fcad40f512578f75c1df3708fe59f248505520a3ef3?mediaT



يظهر في هذا المثال أن المعلن استهدف فئة محددة من الجمهور، وهم محبو المغامرات وخبراء الثقافة الفنون، ومحبو الذهاب إلى الشاطئ والركمجة، وخبراء التجميل، ومحبو الكتب والقراءة، وطلبة الجامعات، ومحبو الطعام، والهيبسترز، ومؤثرو الموضة، ومتابعو الأخبار السياسية، ومحبو الرحلات والطبيعة، ومحبو الحيوانات البرية والأليفة، ومحبو الأعمال الخيرية، والرحالة، ومتابعو موضة المرأة".

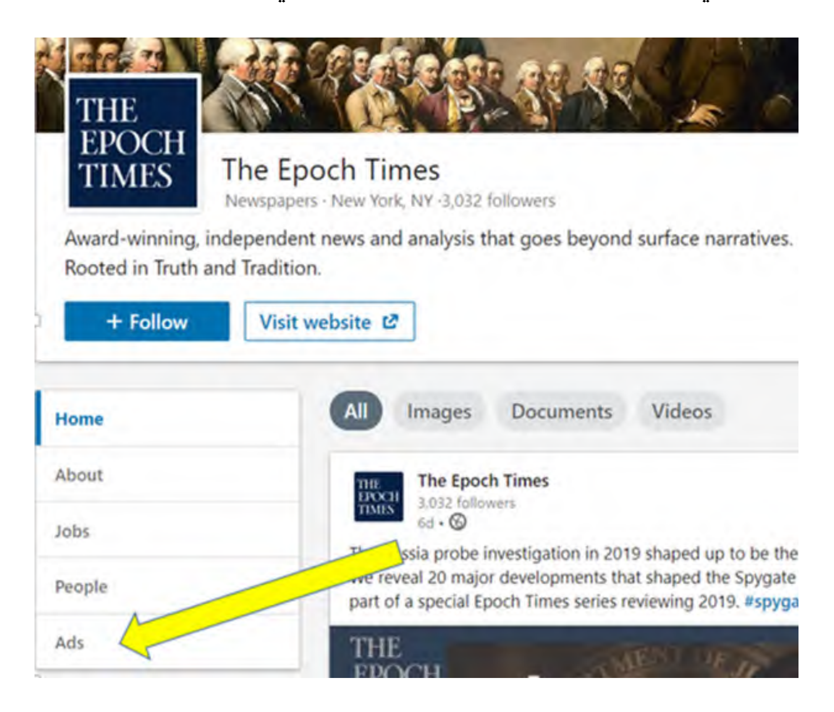
أما المنصات الأخرى فلا توفر هذا القدر من المعلومات بخصوص فئات المستخدمين المستهدفة في الإعلانات.

كما ستجد في جدول البيانات رابطًا ينقلك إلى الإعلان. في هذا المثال وجدت أن الإعلان يتضمن رسالة تشجع الناس على طلب أعلام "قوس قزح" لتصلها بشكل مجاني، وذلك لحشد الدعم لاستفتاء في سويسرا يتعلق بإنهاء التمييز ضد المثليين.

لينكد إن

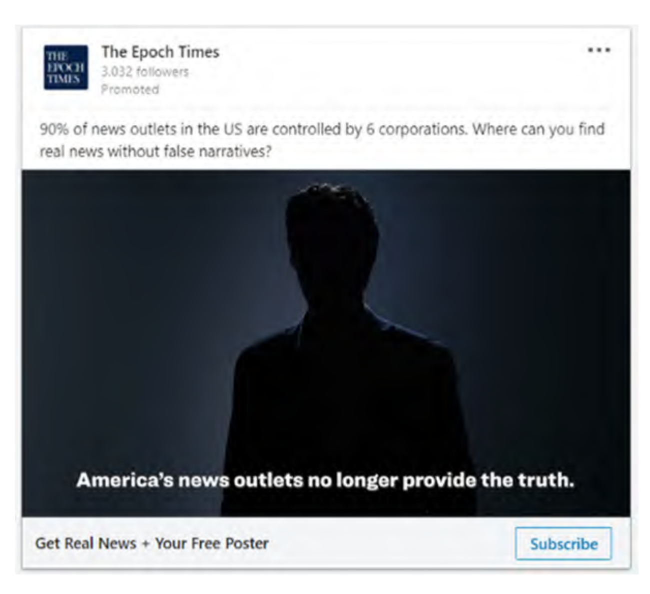
الإعلانات السياسية غير مسموحة على منصة لينكد إن، كما لا توجد مكتبة للإعلانات فيها. لكن هنالك طريقة يمكن اتباعها من أجل الوصول للمعلومات الخاصة بإعلانات شركة محددة على المنصة.

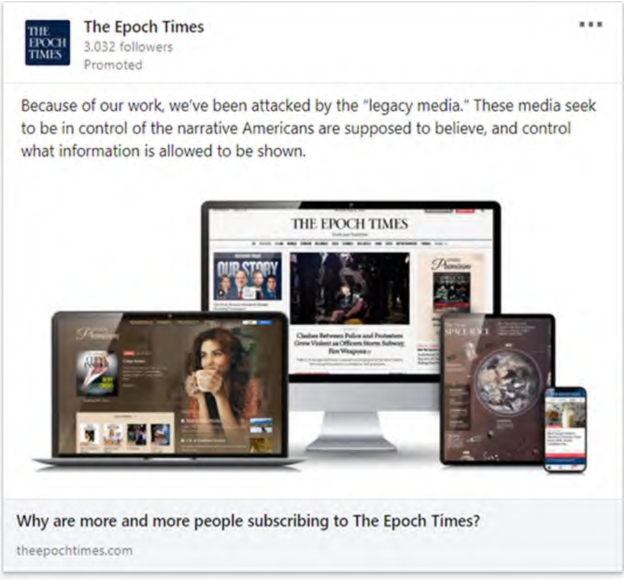
اذهب إلى صفحة الشركة التي تبحث عنها على لينكد إن، وستجد قسم "الإعلانات" في أسفل العمود على اليسار كما يظهر في الصورة أدناه:



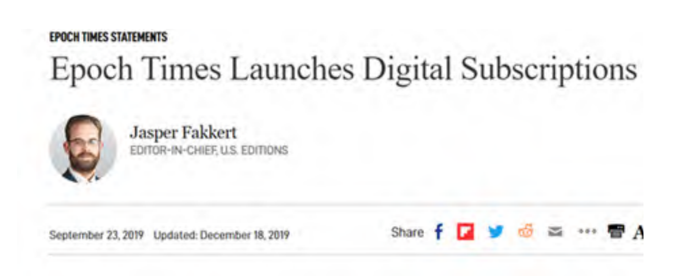
عند النقر على خيار "الإعلانات" ستظهر لك قائمة بجميع الإعلانات

التـي نشـرتها تلـك الشـركة فـي الأشـهر السـتة الماضيـة. وقـد تمكنّـا عبـر ذلـك مـن اكتشـاف أن Epoch Times كانـت مـا تـزال تنشـر إعلاناتهـا علـى لينكـد إن حتـى بعـد أن منعـت مـن الإعـلان فـي فيسـبوك. وكانـت المنشـورات التـي موّلتهـا هـذه الشـركة تدّعـي أن وسـائل الإعـلام الأمريكيـة لـم تعـد تنقـل الحقيقـة، مـع الإشـارة فـي المقابـل إلـى أن "إيبـوك تايمـز" هـي وسـيلة الإعـلام "المستقلة" و "غير المتحيّزة".





لا تظهر تواريخ النشر الخاصة بهذه الإعلانات، ولكن يمكن عبر النقر على رابط الإعلان نفسه (والذي سيظهر حتى لو لم يعد الإعلان فعالًا على لينكد إن)، لتصل إلى التاريخ الدقيق للمنشور. في الإعلان الأول كان الإعلان لمادة منشورة في 23 سبتمبر 2019، وتم تحديثها في 18 ديسمبر 2019، وهذا يساعد على تقدير الفترة التي كان فيها الإعلان فعالًا.


EPOCH TIMES STATEMENTS
Epoch Times Launches Digital Subscriptions
Jasper Fakkert
EDITOR-IN-CHIEF, U.S. EDITIONS
September 23, 2019 Updated: December 18, 2019
Share

يمكن أن تكون مكتبات الإعلانات عنصرًا بالغ الأهمية في التحقيق الرقمي الذي تقوم به، خاصة عند اكتساب مهارة أكبر في التعامل معها والاستفادة من مزاياها الخفية، ولا بدّ للصحفي أن يعود إليها عند التحقق من شخص أو هيئة لها وجود على منصات التواصل الاجتماعي.

الفصل العاشر: التعقب عبر منصات التواصل الاجتماعي

بين كولينز

بين كولينز: مراسل شبكة "إن بي سي" الإخبارية مختص بتغطية القصص الصحفية المتعلقة بالمعلومات المضللة والتطرف والإنترنت. وقد أعد كولينز خلال السنوات الخمس الماضية العديد من التقارير حول رواج نظريات المؤامرة، ومجتمعات الكراهية، وحملات التلاعب من قِبل جهات أجنبية، وحالات الإخفاق في منصات التواصل الاجتماعي. كما عمل كولينز سابقًا مع موقع "ديلي بيست" الأمريكي، وقد تمكن مع فريق من الصحفيين من الكشف عن تورط لجان إلكترونية -تابعة لوكالة أبحاث الإنترنت الروسية- في إنشاء حسابات ومجموعات رقمية وفعاليات واقعية إبّان الانتخابات الأمريكية عام 2016.

في 3 أغسطس 2019، دخل باتريك كروسيوس إلى متجر وول مارت في إل باسو وقتل 22 شخصًا في هجوم له دوافع عنصرية قام به شخص يميني متطرف. لكن قبل أن يتوجّه هذا الشاب إلى المتجر، كان قد نشر بيانًا على قسم المنتدى السياسي في 8chan.net، وهو موقع لتبادل الرسائل مجهولة الأسماء بات مؤخرًا يستخدم بشكل أساسي كنقطة للتواصل بين العنصريين البيض، ولا يخضع هذا الموقع، ولا موقع 4chan الشبيه إلى أي شكل من الرقابة على المحتوى فيهما. وقد أصبح موقع 8chan في صيف 2019 مرتعًا للتواصل بين القوميين البيض المتطرفين ونشر محتواهم.

ونظـرًا لذلـك يقـوم بعـض مسـتخدمي 8chan أحيانًـا بتنبيـه السـلطات والصحفييـن فـي حـال نشـر بيـان جديـد يشـتمل علـى تهديـد أو خطـة لارتـكاب أعمـال عنـف، وذلـك عبـر كتابـة تعليقـات علـى البيـان نفسـه أو عبـر التواصل المباشـر مـع الإعـلام أو الجهـات الأمنيـة المختصـة. وحيـن قـام منفـذ الهجـوم فـي إل باسـو بكتابـة منشـور علـى الموقـع، والـذي تضمّـن فـي البدايـة مرفقًـا خاطئًـا، علـق أحـد المسـتخدمين بقولـه: "Hello FBI". ثـم قـام منفـذ الهجـوم بنشـر المرفـق الصحيـح للبيـان أسـفل التعليـق الـذي حـاول تنبيـه مكتـب التحقيقات الفيدرالي.

هـذا النـوع مـن التبليـغ الذاتـي يشـكل أهميـة خاصـة للصحفييـن خاصـة حيـن يتعلـق الأمـر بمثـل هـذا النـوع مـن الحـوادث المأسـاوية. وقـد يقـوم بعـض المسـتخدمين الأكثـر جـرأة أحيانًـا بالتحذيـر مـن بيـان مـا أو عمليـة عنـف محتملـة عبـر المنصـات المعروفـة علـى الشـبكة، مثـل ريديـت أو تويتـر، وهـذا أمـر ضـروري نظـرًا إلـى سـهولة عـدم ملاحظـة مثـل هـذه الأنشـطة والتعليقات على 4chan أو 8chan.

وإن للمنصـات التـي تتيـح خاصيـة النشـر بـدون تعريـف مثـل 4chan و8chan دورا كبيـرا فـي منظومـة نشـر المعلومـات الزائفـة والمضللـة، وذلـك لأنهـا مسـاحات تتيـح للآخريـن عـادة العمـل عبرهـا لتنسـيق حمـلات التضليـل. كمـا تعـدّ ريديـت أيضًـا مـن المنصـات المشـهورة التـي يلجـأ إليهـا المسـتخدمون للنشـر بـدون أسـماء، وفيهـا نطـاق واسـع ومتنـوع مـن المجتمعـات الرقميـة المختلفـة، حيـث يتشـارك بعـض المسـتخدمين فـي بعضهـا قصصًـا عاديـة عـن هواياتهـم واهتماماتهـم ويناقشـون فيهـا الأخبـار والأحـداث، ولكنهـا توفّـر فـي المقابـل مجـالًا للبعـض لتـداول الكراهيـة دون أي ضابـط. ومـن الضـروري أن يعـرف الصحفـي الكيفيـة الأسـلم لمراقبـة هـذه المجتمعـات الرقميـة المختلفـة ومعرفـة الأسـاليب المتعلقـة بعملها.

وفيما يلي خمسة قواعد على الصحفي الالتزام بها عند الاضطرار لاستخدام موقع 4chan أو 8chan (أو الموقع الجديد البديل 8kun) لأغراض تتعلق بعمله الصحفي:

1. لا تثق بأي شيء متداول في 4chan/8chan
2. لا تثق بأي شيء متداول في 4chan/8chan
3. لا تثق بأي شيء متداول في 4chan/8chan
4. قد تجد بعض المعلومات المفيدة حول جريمة ما أو حملة تضليل أو استهداف رقمية
5. لا تثق بأي شيء متداول في 4chan/8chan

الفكرة هنا هي التأكيد قدر الإمكان على أهمية اتباع القواعد 1 و2 و3 و5، حتى لو منعك ذلك من الاستفادة من بعض المعلومات المغرية كما أوضحنا في النقطة 4. فهذه المواقع قد أنشئت أصلًا من أجل التضليل ونشر المعلومات الزائفة عن "أعداء" مفترضين، والترويج لأكاذيب عن المجتمعات المهمشة، وأحيانًا ما يمتزج ذلك بنشر أكاذيب على شكل نكات في قالب قصص حقيقية عن حياة المراهقين.

وهذا ما يجعل مثل هذه المواقع "مكبّات" إلكترونية لنشر البيانات من قبل المتطرفين البيض والمحبطين جنسيًّا وغيرهم.

ولا بد -مجددًا- من التأكيد على ضرورة عدم استبعاد أن يكون أي شيء ينشر على 4chan أو 8chan (وسنقتصر من الآن فصاعدًا على استخدام 8chan للإشارة إليها جميعًا) محضَ كذب يُقصد منه بث الفوضى وتضليل الصحفيين؛ لذا تجنب التعليق على المنشورات هناك طلبًا للمزيد من التفاصيل، بل تجنب نشر أي شيء، وإلا فإنك ستصبح هدفًا لرواد مثل هذه المواقع الذين لديهم ما يكفي من الوقت والفراغ.

التأكد من المانفستو

الفائدة المرجوّة الأساسية من مواقع مثل 8chan تكمن في محاولة أعضاء من هذا المجتمع الإلكتروني نفسه بالتحذير من مانفستو ما أو الإشارة إلى محتوى ذي قيمة إخبارية حقيقية.

لقد كان تعليق أحدهم عبر كتابة "Hello FBI" على موقع 8chan هو ما ساعدني على التوصل إلى مانفستو منفذ الهجوم في إل باسو. وبعد فترة قصيرة من الحادثة، بحثت على تويتر عن (El Paso 8chan) و (El Paso 4chan)، وهي الطريقة التي أستخدمها للبحث عن أي معلومات تتعلق بحوادث أخرى قد تكون مرتبطة بأشخاص يرتادون مثل هذه المواقع ولهم نشاط عليها.

كشفت عملية البحث التي أجريتها على تويتر عن وجود عدد من المستخدمين الذين شاركوا لقطات شاشة (Screenshots) تتضمن منشورات منفذ الهجوم على 8chan، مع أن العديد منهم نسبوها إلى مستخدم آخر على 4chan، ولذا كان عليَّ أن أتأكد من المنشور ومكان وجوده.

لكن ما هي الطريقة الأسرع للبحث عن منشور في 8chan؟ الجواب: جوجل.

في أعقاب الهجوم في إل باسو، بحثت في جوجل باستخدام عبارة "site:8chan.net"، ثم أضفت جزءًا من جملة من المنشور المزعوم الذي نشره منفذ الهجوم على 8chan. (تنبه إلى أن موقع 4chan يحذف المنشورات عن خوادمه بعد فترة من الزمن، لكن يمكنك أن تعثر على مواقع تؤرشف محتوى الموقع بشكل تلقائي، وأهمها هو موقع 4plebs.org، ويمكن الوصول إلى المنشور المحذوف بكل بساطة عبر كتابة 4plebs مكان 4chan في الرابط الخاص بالمنشور المحذوف،

وحذف السابقة "boards". على سبيل المثال: /boards.4chan.org pol/13561062.html تصبح 4plebs.org/pol/13561062.html وهكذا ستصل إلى المنشور المطلوب حتى لو كان محذوفًا عن الموقع الأصلي).

وقد يكون من الجيد في بعض الحوادث المتعلقة بهجمات إطلاق نار البحث عبر استخدام عبارة: ”site:4chan.net + ‘manifesto’ or fbi‘‘ واستخدام خيارات البحث في جوجل لتحديد البحث بفترة 24 ساعة ماضية فقط. فمن الممكن أن يكون بعض المستخدمين في الموقع قد حاولوا أن يبلّغوا عن منفذ الهجوم في منشوراتهم.

ولم أتمكن في عملية البحث الأولية التي قمت بها من التوصل إلى المنشور المطلوب في 8chan، ما جعلني أفترض أنه قد يكون مجرد منشور فبركهُ أحدُهم بشكل سريع على الموقع. لكن الغريب هو أن المنشور الذي ظهر على لقطات شاشة على تويتر كان يتضمن رقم تعريف بصاحب المنشور ورقمًا للمنشور أيضًا. وقد دفعتني هذه التفاصيل إلى الاقتناع بأن المنشور حقيقي وليس مجرد فبركة.

كل منشور على موقع 8chan له رقم تعريفي (ID)، يتم توليده وفق خوارزمية محددة ويظهر بجانب تاريخ كل منشور، وهو نظام يتيح للمستخدم أيضًا أن يكون له رقم تعريف ثابت كي يميز كلٌّ مستخدم نفسه في سلسلة من المنشورات.

هذا النظام التعريفي بالمستخدم هو ما يسمح بالربط بين منشور معين ورقم المستخدم الذي نشره، فالمستخدمون على مثل هذه المواقع يقومون بإنشاء أسماء مستخدم ثابتة فعليًا بكلمات مرور يختارونها، حيث يقوم بإدخال اسم المستخدم في خانة الرقم التعريفي عند كتابة منشور ما، ويتبعه بعلامة الوسم (#)، ثم كلمة المرور.

وعبر هذا الرقم التعريفي تمكنت من معرفة أن الشخص الذي نشر

بالخطأ وثيقة البي دي أف التي اشتملت على اسم منفذ الهجوم، كان هو الشخص ذاته الذي نشر المانفستو بعد دقيقتين من المنشور السابق، فكلا المنشورين حملا الرقم التعريفي: 58820b.

وإلى جانب الرقم التعريفي للمستخدم يظهر الرقم التعريفي بالمنشور، وهو ما يستخدم من أجل توليد رابط منفصل خاص بكل منشور. لقد كانت لقطة الشاشة من مانفستو إل باسو والتي انتشرت على تويتر تحمل رقم المنشور: No. 13561062، وهذا يعني أن رابط المنشور على 8chan هو: 8ch.net/pol/res/13561062.html. لكن في حالتنا هذه لم يكن المنشور موجودًا، ما دفعني لافتراض أنه ربما يكون قد حذف (وقد علمت لاحقًا أن مالك موقع 8chan، جيم واتكينز، قد حذف المنشور فور أن وصله تنبيه بشأن محتواه).

بعد أن تبين أن المنشور محذوف لم يبق لديّ سوى أمل وحيد بأن يكون هنالك شخص ما قد تنبّه لأهميته وعمل على أرشفته. ولحسن الحظ، ثمة مستخدم سريع البديهة على 8chan قام بحفظ المنشور على archive.is. وعند لصق الرابط الخاص بالمنشور في خانة البحث في موقع الأرشيف، تأكدت من أن المنشور الخاص بالمانفستو كان حقيقيًا، وبوسعي الآن أن أطلع عليه بشكل مباشر من النسخة المؤرشفة منه.

لكني اصطدمت بعد ذلك بمشكلة أخرى، وهي مسألة الوقت الذي نشر فيه المانفستو على 8chan. لقد كنت بحاجة إلى ما يدلّ بشكل واضح على وقت النشر للجزم بأن المنشور قد ظهر قبل تنفيذ الهجوم في إل باسو.

تقوم المواقع مثل 4chan و8chan بتعقيد عملية نقل التاريخ والوقت الخاص بالمنشورات عند أرشفتها على مواقع أخرى، لكن هنالك لحسن الحظ طريقة لتجاوز ذلك. انقر (Right-Click) على الختم الزمني (Timestamp)، ثم اختر (Inspect Element)، لتعرض الكود المصدري الخاص بالموقع، وسيظهر قسم يبدأ بدلالة الوقت <time’ unixtime=‘[number]. بحيث يظهر رقم داخل الهلالين.

انسخ هذا الرقم وابحث عنه في أحد المواقع الخاصة بتحويل الأختام الزمنية مثل unixtimestamp.com، وستحصل على ختم زمني دقيق للمنشور بالتوقيت العالمي المنسق (UTC). وبعد تحويل الوقت من التوقيت العالمي المنسق إلى التوقيت في إل باسو، تبين أن المانفستو كان قد نشر في الساعة 10:15 صباحًا حسب توقيت إل باسو، أي قبل دقائق من تنفيذ عملية إطلاق النار في المتجر.

لقد ساعدتني هذه العملية على تأكيد أن المانفستو الذي نشر على 8chan كان في الواقع دليلًا حقيقيًا في حادثة إرهاب محلي ذات دوافع عنصرية.

تعقب المستخدمين عبر المنصات

في عام 2017، قام شخص يُدعى لاين ديفيز، والذي كان متورطًا في حملات مضايقة إلكترونية، مثل حملة "غيمرغيت" سيئة الصيت، بقتل والده، بسبب جدال حول ميلو يانوبولوس، أحد رموز اليمين المتطرف في المملكة المتحدة.

بدأ جدال وتلاسن شديد بين ديفيز ووالده، وأظهر تسجيل مكالمة مع النجدة بأن ديفيز كان يتلفظ بعبارات عنصرية متطرفة متداولة بين أنصار اليمين المتطرف على الإنترنت، قبل الهجوم على والده. نعت ديفيز والديه بأنهما من "اليساريين المتحرشين بالأطفال"، وذلك قبل أن يتصل والده بالشرطة ليطلب منهم طرده من منزله حيث كان يعيش معهما.

كان ديفيز معروفًا باسم "Seattle4Truth" على الإنترنت، وقد ظهر في عدد من مقاطع الفيديو على يوتيوب لينشر معلومات زائفة عن مجموعات سرية من المتحرشين بالأطفال والذين يدّعي أنهم هم القوّة المحرّكة للتيار الليبرالي، حتى إن أحد فيديوهاته على يوتيوب حمل عنوان "الأدلة الواضحة على الارتباط بين الأيديولوجيا التقدمية والبيدوفيليا".

ومـن المعـروف أن حلـم أي صحفـي يعمـل علـى تحقيـق يتعلـق بالتطـرف علـى الإنترنـت هـو أن يكـون الشـخص -موضـوعُ التحقيـق- يعتمـد علـى اسـم مسـتخدم واحـد فـي المنصـات المختلفـة التـي ينشـط عليهـا، وقـد كان هـذا هـو الحــال مــع لايــن ديفيــز، الــذي التــزم باســم مســتخدم فريــد هــو Seat-tle4Truth علـى يوتيـوب وعلـى ريديـت، حيـث تكشـف منشـوراته بوضـوح عن العقلية المؤامراتية المسكون بها.

وقـد تـم اكتشـاف لايـن ديفيـز علـى ريديـت بـكل بسـاطة عبـر إضافـة اسـم المســتخدم Seattle4Truth علــى الرابــط الخــاص باســم المســتخدم فــي ريديــت وهــو: reddit.com/u/[username]. بعــد إدخــال الاســم والوصـول إلـى الحسـاب، سـيكون بوسـعك البحـث بأكثـر مـن طريقـة، عبـر فلتـرة المنشـورات مـن الأحـدث إلـى الأقـدم، أو المنشـورات الأكثـر تفاعـلًا، أو المنشــورات "الأكثــر إثــارة للجــدل"، والتــي تعــرض المنشــورات التــي نالت الكثير من الإعجابات وقدرًا قريبًا من عدم الإعجاب أو العكس.

ويمكـن البحـث عـن اسـم المسـتخدم بسـرعة عبـر اسـتخدام أداة Namechk، والتــي تســاعدك فــي البحــث عــن اســم مســتخدمٍ مــا علــى أكثــر مــن 100 منصــة رقميــة علــى الإنترنــت. لكــن مــن الضــروري التنبّــه إلــى أنّ هــذا لا يعنــي أن اســم المســتخدم المتكــرر علــى أكثــر مــن منصّــة تُــدار مــن قبــل شـخص واحـد، لكنهـا طريقـة جيـدة تسـاعد علـى تحديـد المنصـات التـي يـرد فيهـا هـذا الاسـم، كخطـوة عمليـة أولـى يلزمهـا المزيـد مـن التحـري والبحـث. كمـا يمكنـك دومًـا الاسـتفادة مـن محـرك البحـث جوجـل للبحـث عـن أي اسـم مستخدم آخر.

مـن الضـروري كذلـك مراعـاة وجـود بعـض المجتمعـات الرقميـة الحصريـة التــي يمكــن أن ينشــط فيهــا الشــخص المســتهدف فــي عمليــة البحــث التــي تجريها.

ففــي العــام 2017 كان ويليــام إدوارد أتشيســون، منفـذ هجـوم إطـلاق النـار عـام 2017 فـي إحـدى المـدارس فـي نيومكسـيكو، نشـطًا علـى موقـع -Kiwi

Farms، وهو متوقع متخصص في التنمّر على الأشخاص المتحولين جنسيًا، حيث كان موجودًا على الموقع باسم مستخدم @satanicdrug-gie. كما أفاد بعض المستخدمين بأنه كان نشطًا على موقع Encyclo-pedia Dramatica، وهو موقع لتجميع الميمز وينشر أحيانًا محتوى متطرفًا. ولم يكن أتشيسون عضوًا في هذا الموقع وحسب، بل كان مشرفًا وله صفة إدارية فيه. وقد أكّد لنا عدد من مستخدمي الموقع، والذين كانت تربطهم علاقات مباشرة عبر سكايب مع أتشيسون، بأن الحسابات كانت له بالفعل. كما ذكروا أن أتشيسون كثيرًا ما كان يبادر ويخبر المستخدمين عن حسابات أخرى تابعة له يستخدمها بشكل احتياطي في حال تعرّض حسابه الرئيسي للحظر. وقد بحثت عن اسم المستخدم الخاص به على جوجل عبر صيغة البحث:

"site:encyclopediadramatica.rs + [username]"، وقد تبين أنه كان يعتمد اسم المستخدم "Satanic Druggie"، إضافة إلى أسماء أخرى مثل "Future School Shooter"، و"Adam Lanza"، وهذا الأخير هو اسم منفذ هجوم إطلاق النار في مدرسة ساندي هوك عام 2012.

ومن خلال النظر في تاريخ منشوراته عبر المنصات المختلفة يظهر لنا مقدار هوس هذا الشخص بهجمات إطلاق النار في المدارس، وهي منشورات لم يتمكن حتى رجال الشرطة من التوصل إليها أثناء التحقيقات التي تلت الهجوم الذي نفّذه.

ويلزم أن نؤكد مجددًا هنا على أن وجود اسم مستخدم مشترك على أكثر من منصّة لا يضمن بالضرورة أن تكون الحسابات كلها تابعة للشخص عينه. ومن الأمثلة التي تذكر في هذا السياق هو ما ادّعته بعض الشخصيات سيئة الذكر من اليمين المتطرف والناشطين في نشر المعلومات المضللة، والذين ادّعوا أن من قتل شخصين وجرح عشرة آخرين في بطولة لألعاب الفيديو في جاكسونفيل كان شخصًا مناهضًا للرئيس الأمريكي دونالد ترمب.

أما السبب الذي قدموه فهو أن منفذ الهجوم، ديفيد كاتز (David Katz)، ينشط باسم المستخدم (Ravens2012Champs) في بطولات ألعاب الفيديو، وأنهم وجدوا حسابًا مناهضًا على ريديت في تويتر باسم المستخدم (RavensChamps). وقد تمّ ترويج هذه القصّة في حملة شعواء رغم زيف المعلومات التي تنقلها، ونشر أحد هذه المواقع اليمينية المتطرفة مقالًا أفاد عنوانه بأن مطلق النار في جاكسونفيل انتقد أنصار ترمب على ريديت، وادّعى المقال أن منفذ الهجوم كان كارهًا لترمب.

لكن الواقع كما تبيّن هو أنهما شخصان مختلفان، وأن الحساب الثاني على ريديت هو لعامل مصنع في مينيسوتا يدعى بافل، والذي كتب على حسابه في ريديت بعد الحادثة: "أنا ما زلت حيًا، صدقوني"، ليؤكّد لأصدقائه أنه ليس الشخص الذي نفّذ الهجوم، والذي قتل نفسه أيضًا بعد المجزرة.

لذلك فإن الاشتراك باسم المستخدم لا يكفي للجزم بأن الحسابات تتبع لشخص واحد، ولكنها إشارة أولية وحسب، يمكن الانطلاق منها للمزيد من التحري والتأكّد بشكل قاطع.

وقد يستلزم ذلك من الصحفي البحث بشكل معمق في السجلات والتواصل مع الآخرين وإرسال بعض الرسائل أو إجراء بعض المكالمات.

تعقب الحملات بشكل شبه تزامني

عادة ما تنتشر حملات التضليل والتلاعب الإعلامي في وقت متزامن على منصة ريديت و4chan، ويمكن تعقب بعضها أحيانًا بشكل تزامني.

فعلى سبيل المثال، ينشط موقع 4chan منذ سنوات في فبركة استطلاعات رأي من أجل دعم مرشحين بعينهم على حساب آخرين. وفي عام 2016، قام مستخدمون على 4chan وبشكل مكثف بنشر

روابط على مواقع إخبارية وطنية ومحلية تشتمل على طلبات للمشاركة في عمليات استطلاع رأي إلكترونية في سياق مناظرات انتخابية يشارك فيها المرشّح المفضّل لمستخدمي الموقع، وهو دونالد ترمب.

عبر البحث في جوجل باستخدام الصيغة: ("'site:4chan.org 'polls") وفلترة نتائج البحث؛ بحيث تظهر لك المنشورات في الساعة الماضية فقط عبر خيار "last hour"، فستكون لديك فكرة جيدة عن الاستطلاعات التي يرغب مستخدمو موقع 4chan في التلاعب بها بالوقت الحقيقي.

وقد استمر هذا النمط من محاولة التأثير في هذه الاستطلاعات في الدورة الثانية من الانتخابات، حيث دعم مستخدمو الموقع تولسي غابارد، والتي أطلقوا عليها لقب "ماما" (Mommy)، وذلك في استطلاعات قامت بها مواقع مثل Drudge Report وNJ.com.

وعبر استخدام صيغة البحث نفسها على جوجل، يمكن ملاحظة التغير الذي يطرأ في الوقت الحقيقي على نتائج الاستطلاع بعد ظهور منشور على الموقع من أحد المستخدمين يدعو فيه الآخرين إلى دعم المرشّحة "بكل ما أوتيتم من قوة".

ومن السهل أيضًا ملاحظة مثل هذا النشاط المنظم على مواقع أخرى مثل "ريديت" في منتدياته الفرعية، مثل (r/The_Donald)، وذلك بفضل ميزة تصدير المنشورات الأكثر تفاعلًا في ريديت.

عبر استخدام الصيغة ("-reddit.com/r/[subreddit-name]/ris ing") يمكنك استعراض نتائج تحظى بتفاعل كبير في منتدى فرعي على ريديت وفي أي ساعة، كما يمكنك النظر في المنشورات ذات النشاط الفائق عبر منصة ريديت بأكملها عبر reddit.com/r/all/ris-ing، حيث يمكنك الاطلاع على كافة المنشورات الأكثر رواجًا وتفاعلًا في غالبية المنتديات الفرعية في ريديت، باستثناء المنتديات الفرعية "المحجورة"، وهي المجتمعات الرقمية المسيئة على ريديت، والتي ينشر

فيها محتوى مهين أو عنصري في حملات منظمة.

كما لا تظهر هذه المنتديات الفرعية على جوجل، ولكن يمكن البحث فيها عبر الصيغة: (“reddit.com/r/[subreddit-name]/rising”). ومع أن فرض "الحجر" على مثل هذه المنتديات الفرعية يمنع وصول المحتوى الذي ينشر بها خارج الدوائر الضيقة الخاصة بها من المتابعين، إلا أن ذلك يجعل من الصعب تتبع أنشطة بعض الأطراف الذين يستغلون هذه المساحات لتنظيم أنفسهم.

يمكن القول إجمالًا: إنه من الضروري متابعة هذه المساحات الرقمية ذات الرواج المتزايد بين المستخدمين الناشطين في حملات التضليل والتلاعب، مثل المنتدى الفرعي على ريديت الخاص بأنصار ترمب (r/The_Donald)، ولاسيما في سياق الأحداث الكبرى مثل الانتخابات أو المناظرات السياسية أو في سياق أي هجمات أو حوادث عنف.

كما يلزم التنبه إلى أن ما تقوم به بعض المنصات من تقييد وصول المحتوى السلبي الذي ينشره بعض المستخدمين عليها قد يزيد من صعوبة مهمة الصحفي في الحصول على معلومات أساسية. ومع أن بعض الأدوات قد تساعده في تجاوز ذلك، إلا أن ذلك يتطلب الكثير من الجهد والوقت، ويتطلب الالتزام بمنهجياتٍ تحقُّق خاصة، قد لا تستطيع الخوارزميات وأجهزة الحاسوب إعادة إنتاجها، ولا بدّ في النهاية من تدخّل الصحفيّ نفسه للوصول إلى النتائج المطلوبة.

الفصل الحادي عشر: تحليل الشبكات والكشف عنها

بين نيمو

بين نيمو: مدير قسم التحقيقات في مؤسسة Graphika وباحث أول غير مقيم في مختبر أبحاث التحقيقات الرقمية في المجلس الأطلنطي (Digital Forensic Research Lab)، وهو متخصص في دراسة التأثير الإعلامي ونشر المعلومات في الحملات الكبيرة التي تنفذ على أكثر من منصّة. نيمو من محبّي الغوص تحت الماء، حيث لا يمكن الوصول إليه عبر الهاتف.

عند التعامل مع أي عملية مريبة تتعلق بالتلاعب الإعلامي والتأثير، فإن السؤال الأبرز الذي يرد على ذهن الباحث هو ذلك المتعلق بحجم هذه العملية ونطاق انتشارها. وهذا سؤال يختلف عن تقييم التأثير الذي تحققه العملية والذي يتطلب مساحة أخرى من التحري والبحث.

أما السؤال الأول فيتعلق بتحديد الحسابات والمواقع الإلكترونية التي تقف وراء الحملة نفسها. فالهدف بالنسبة للمحقق الصحفي هو الكشف عن العملية نفسها ونقاط نشاطها وانتشارها وتأثيرها، وذلك قبل نشر تقريره حولها، والسبب هو أنه بمجرّد نشر التقرير الخاصة بحملة مشبوهة ما؛ فإن المسؤولين عنها سيقومون عادة بوقف نشاطهم، عبر حذف بعض الحسابات أو إغلاق المواقع التي لم يتم الكشف عنها والتعمية على أي أثر آخر قد يكشف عن الحجم الحقيقي للعملية.

الحلقة الأولى في السلسلة

يعدّ الوصول إلى "طرف الخيط" أحد أصعب المراحل في أي عملية تحقيق. في كثير من الأحيان قد يبدأ التحقيق من إشارة يرسل بها أحد المستخدمين في موقع ما أو ربما (وإن كان ذلك نادرًا) من منصات التواصل الاجتماعي.

فمثلًا، اعتمد التحقيق الذي قام به مختبر أبحاث التحقيقات الرقمية (DFRL) للكشف عن عملية تضليل روسية عرفت باسم "Second-ary Infektion"، على معلومات سريّة أولية من داخل فيسبوك، والتي لاحظت وجود 21 حسابًا مشبوهًا على منصتها. وقد استغرق العمل على إتمام التحقيق فترة ستة أشهر، في جهد مشترك بين غرافيكا ورويترز وريديت، وقد خلص التقرير إلى أنّ هذه العملية كانت تسعى إلى التأثير في الانتخابات البريطانية.

ثمة تحقيق آخر يتعلق بحملة تضليل تستهدف جنودًا سابقين في الجيش الأمريكي، وكان الدافع للشروع به إبلاغ موظف في مؤسسة "المحاربون القدامى في فيتنام" عن وجود مجموعة على فيسبوك تدّعي أنها تمثّل المؤسسة، ولديها من المتابعين عدد يفوق الصفحة الحقيقية التابعة للمؤسسة على المنصة نفسها.

ولا تتوفر قاعدة عامة واحدة تساعد على الإمساك بـ "طرف الخيط" المراوغ، ولكن عادة ما يتطلب ذلك البحثَ في غير المألوف. فقد يكون ذلك حسابًا على تويتر يظهر أن صاحبه في ولاية تينيسي الأمريكية ولكنه مرتبط برقم هاتف روسي، أو صفحة على فيسبوك تدعي أنها من النيجر، ولكنها تدار من السنغال والبرتغال، أو حسابًا على يوتيوب بمشاهدات مليونية تنشر قدرًا كبيرًا من المحتوى الداعم للصين في 2019، ولكن معظم المشاهدات التي حصدها الحساب هي لحلقات من برنامج كوميدي بريطاني تم رفعها عام 2016.

كما قد يكون طرف الخيط المنشود موقعًا إلكترونيًا لا يُعرف من يملكه، ولكنه ينشر محتوى معنيًّا بالسياسة الخارجية الأمريكية، فتكتشف بأنه مسجل باسم الدائرة المالية لمقاطعة الشرق الأقصى العسكرية في الاتحاد الروسي.

كما يمكن أن يكون مقابلة يدّعي من نشرها أنها أجريت مع أحد عناصر جهاز الاستخبارات البريطاني، ولكنه يتكلم بلهجة شكسبيريّة متصنّعة. أو ربما حساب على تويتر يروّج لموقع إباحيّ عبر منشورات تشتمل على اقتباسات مجتزأة من رواية جين أوستن "العقل والعاطفة".

الضروري في كل هذه الأمثلة هو أن تبذل الوقت الكافي لتحليلها والتفكير بها. فكثيرًا ما يشعر الصحفي أو المحقق بقدر من الضغط والعجلة وضيق الوقت بحيث يصرف ذهنه عن متابعة مثل هذه الإشارات المهمّة رغم بساطتها، ولا يجد فيها سوى خطأ شاذٍّ لا يستحق المزيد من التحري، وينسى أن ثمّة سببًا ما وراء حدوث هذا الخطأ.

لذا فإنه من الضروري التأني قليلًا وأخْذ الفرصة الكافية للتفكير بأي نشاط أو ملاحظة مريبة، وطرح السؤال الأولي: لِمَ حصل ذلك؟ وقد تكون الإجابة على ذلك هي الخطوة الأولى في الكشف عن عملية ما.

الأصول، السلوك، المحتوى

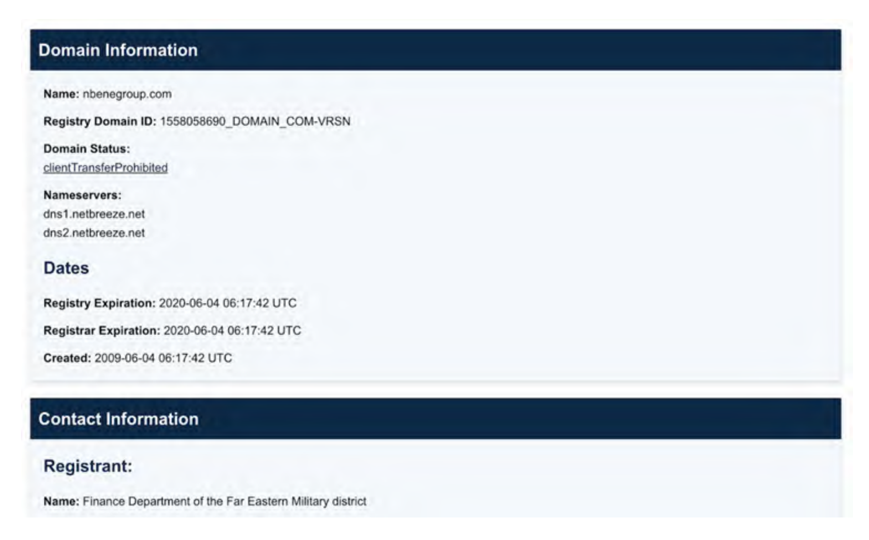
المقصود بالأصول (Assets) هنا هو الحساب أو الموقع الإلكتروني موضوع التحقيق، والذي لا بدّ بعد تحديده من معرفة من يقف وراءه وإلى أين يؤدي.

للنجاح في ذلك يلزمنا في البداية أن نطرح ثلاثة أسئلة أساسية، وهي مصممة على نموذج كاميل فرانسوا الخاص بالكشف عن

المعلومـات المضللة.

- ما المعلومات المتوفرة عن الأصل؟
- ما طبيعة سلوك هذا الأصل؟
- ما المحتوى الذي نشره هذا الأصل؟

تتمثل الخطوة الأولى في جمع أكبر قدر من المعلومات المتعلقة بالأصل الأولي الذي تم تحديده. فإن كان موقعًا إلكترونيا، فلا بد من معرفة متى تم تسجيله، ومن قام بذلك، وتحديد السمات الأبرز للموقع ومتعلقاته الرئيسية، مثل الرقم التعريفي له على أداة جوجل أناليتكس أو جوجل آدسنس، وعنوان البريد الإلكتروني أو رقم الهاتف المستخدم في تسجيل اسم النطاق. ويمكن التوصل إلى إجابات عن كل هذه الأسئلة عبر البحث عنها عبر أدوات عديدة مثل lookup.icann.com أو domaintools.com أو domainbigdata.com أو spyonweb.com.


Domain Information

Name: nbenegroup.com

Registry Domain ID: 1558058690_DOMAIN_COM-VRSN

Domain Status:
clientTransferProhibited

Nameservers:
dns1.netbreeze.net
dns2.netbreeze.net

Dates

Registry Expiration: 2020-06-04 06:17:42 UTC

Registrar Expiration: 2020-06-04 06:17:42 UTC

Created: 2009-06-04 06:17:42 UTC

Contact Information

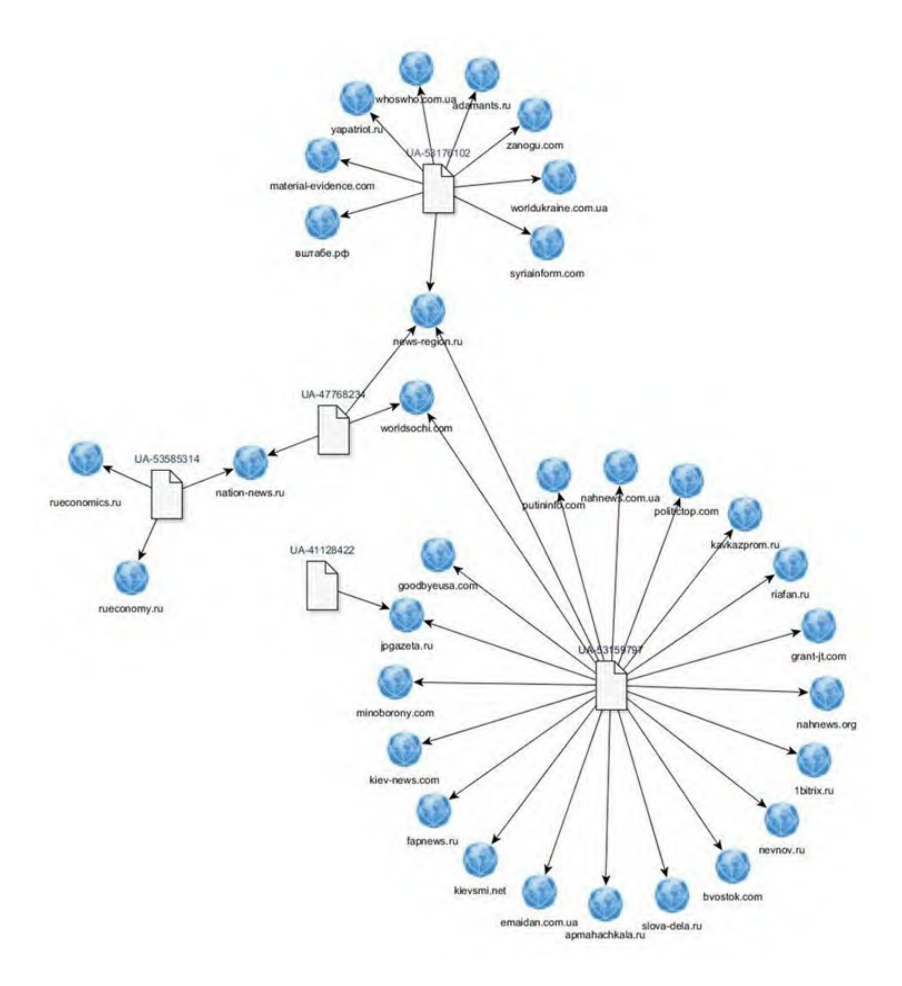
Registrant:

Name: Finance Department of the Far Eastern Military district

تفاصيل تسجيل الموقع الإلكتروني NBeneGroup.com –الذي ادعى أنه مختص بدراسات الشباب– والتي تثبت أن الموقع مسجل باسم قسم المالية لمقاطعة الشرق الأقصى العسكرية في الاتحاد الروسي، وذلك عبر موقع lookup.icann.org.

هذه المعلومات الخاصة بالموقع الإلكتروني مفيدة في عملية البحث عن المزيد من الأصول التي قد تكون مرتبطة به. ويمكن عبر مواقع مثل domaintools.com وspyonweb.com البحث عبر معطيات محددة، مثل عنوان البروتوكول الخاص بالموقع (IP Address) أو الرقم التعريفي بحساب جوجل أناليتكس، وهو ما قد يساعد في التوصل إلى مواقع أخرى مرتبطة بالأصل موضوع البحث، علمًا أن عمليات التلاعب والتضليل الإعلامي الأكثر تعقيدًا في الآونة الأخيرة تحرص على إخفاء المعلومات الخاصة بتسجيل أسماء النطاق في المواقع التي تستخدمها أو استخدام واجهات لهيئات تجارية أو خدمات خاصة، ما يزيد من صعوبة الكشف عن الجهة التي تقف وراء الموقع.

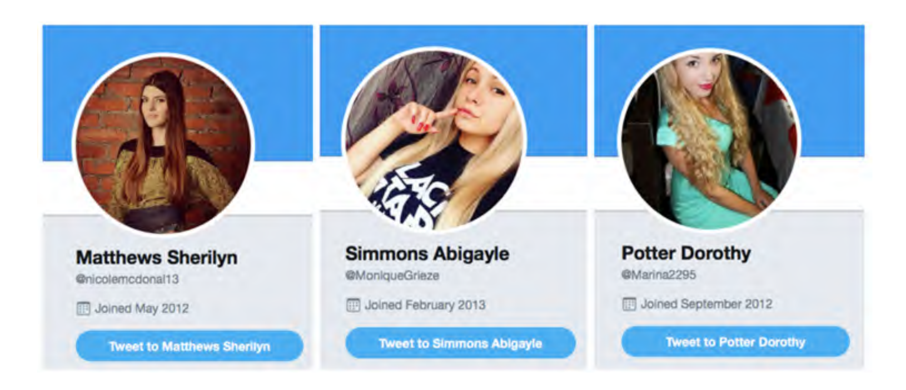
في إحدى عمليات التحقيق التي قام بها الباحث البريطاني لورنس أليكساندر، تبين وجود 19 موقعًا إلكترونيا تدار من قبل وكالة أبحاث الإنترنت الروسية (Russian Internet Research Agency)، وذلك عبر تتبع رقم التعريف الخاص بأداة جوجل أناليتكس. وفي أغسطس 2018، كشفت شركة "فاير آي" (FireEye) المتخصصة بالأمن السيبراني عن عملية تضليل إيرانية واسعة النطاق، وذلك بالاعتماد على معلومات تسجيل أسماء النطاق وعناوين البريد الإلكتروني، ما ساعد في الكشف عن الرابط بين عدة مواقع إلكترونية.



شبكة لعدد من المواقع التي تم الربط بينها عبر تتبع أرقام التعريف الخاصة بحساب جوجل أناليتكس (وهي أرقام من ثماني خانات مسبوقة بالرمز UA).

أما لو كان الأصل المبدئي الذي تم تحديده هو حساب على مواقع التواصل الاجتماعي، فلا بدّ من الاستفادة من العمليات التي تم توضيحها في الفصلين الماضيين بخصوص الكشف عن الحسابات الإلكترونية والمفبركة والتحقق من الحسابات على المنصات المختلفة. ولا بدّ من السؤال عن تاريخ إنشاء الحساب الذي نتحرى عنه، وما إذا كان اسم

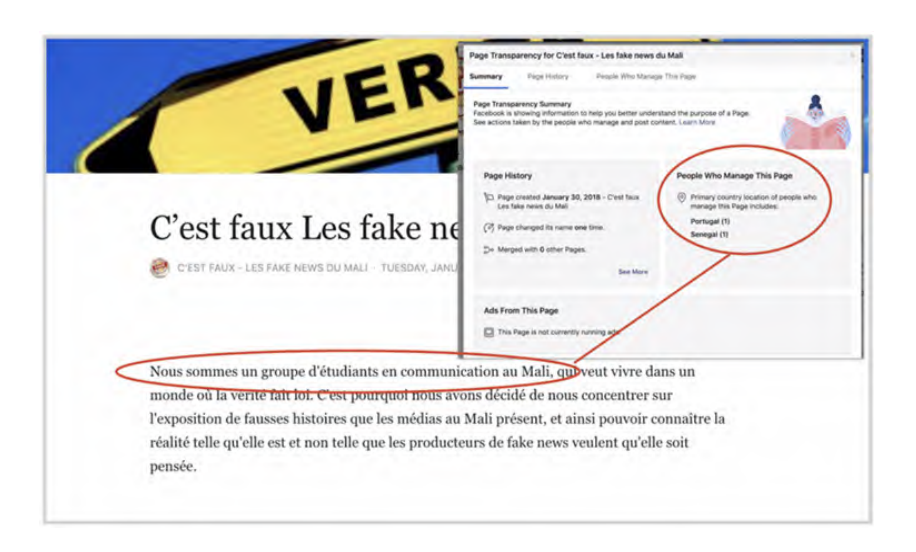
الحساب متطابقًا مع اسم المستخدم، كأن يكون الاسم "Simmons Ab-igayle" واسم المستخدم (الهاندل) هو @moniquegrieze، وهي حالة من شأنها أن تدفعنا إلى الشكّ في احتمال أن يكون الحساب مسروقًا أو مفبركًا.



ثلاثة حسابات متورطة كانت جزءًا من عملية حسابات مزيفة كبيرة في أغسطس 2017. قارن بين أسماء الحسابات وأسماء المستخدم، وكيف أن الفرق بينها يوحي بأنها حسابات مسروقة وأعيدت تسميتها وتغيير مظهرها عبر الجهة التي وظفتها في العملية.

كما يجب ملاحظة ما إذا كان الحساب يوفر معلومات كافية ومعقولة يمكن التثبت من صحتها، أو ما يربطها من حسابات أخرى على المنصة نفسها أو منصات أخرى. أما إن كنت تتعامل مع صفحة أو مجموعة على فيسبوك، فيجب تحديد من يديرها، وذلك عبر الاستفادة من قسم "شفافية الصفحة" على فيسبوك أو التفاصيل الخاصة بأعضاء المجموعة الفيسبوكية، والتي تساعد في التوصل إلى معلومات مهمة.

من الضروري كذلك على تويتر ملاحظة تاريخ إنشاء الحساب، وعدد التغريدات، والإعجابات. (فيسبوك وإنستغرام لا يظهران تاريخ إنشاء الحساب، ولكن يمكن معرفة ذلك تقديريًا عبر الوصول إلى أول منشور أو صورة نشرها صاحب الحساب).



صفحة تابعة لموقع إلكتروني مختص بكشف الأخبار الزائفة، ويدعي أنه يدار من قبل مجموعة من الطلبة في مالي، وتبيّن عبر قسم الشفافية في الصفحة أن الصفحة تدار من البرتغال والسنغال. مصدر الصورة: DFRLab.

وبعد جمع المعلومات الكافية عن الأصل الأولي (الموقع أو الحساب)، ننتقل إلى الخطوة التالية وهي تحليل السلوك الرقمي لهذا الأصل.

والسؤال الذي نطرحه هنا هو: "ما السمات السلوكية الأبرز لهذا الحساب أو الموقع والتي يمكن أن تساعد على ربطها مع حسابات أو مواقع أخرى قد تكون ناشطة في العملية ذاتها؟".

لا شكّ في أن هذا السؤال واسع جدًا، والإجابة عنه تحمل العديد من الأوجه، وبعضها قد لا يتضح إلا في المراحل الأخيرة من التحقيق.

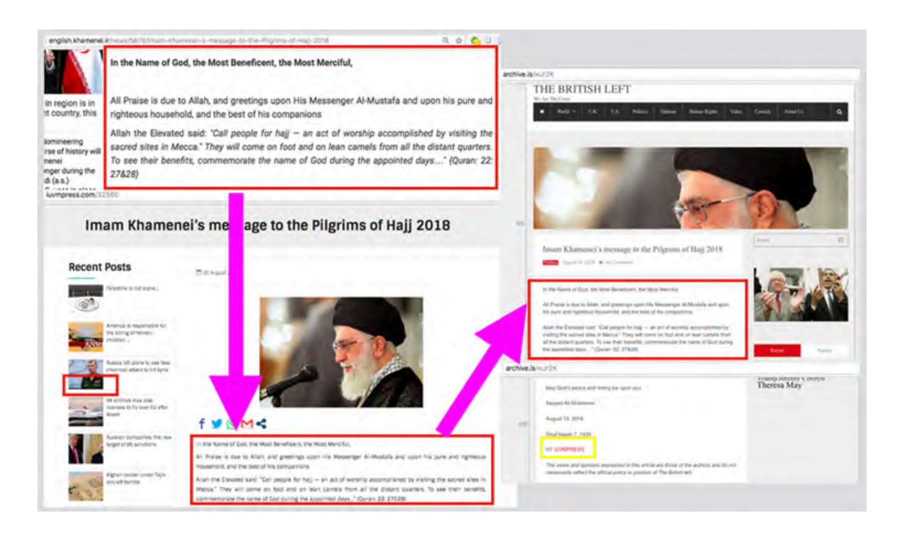
قد يشمل ذلك على سبيل المثال قنوات على يوتيوب بأسماء وصور بروفايل "غربيّة"، ولكنها تنشر مقاطع فيديو سياسية باللغة الصينية، من بين أعداد كبيرة من مقاطع فيديو قصيرة من تيك توك.

كما قد تشتمل على شبكات من الحسابات على فيسبوك وتويتر والتي

تنشط في نشر روابط لمحتوى من موقع واحد أو مجموعة واحدة من المواقع، أو حسابات ذات نبذ تعريفية (bio) متشابهة بشكل حرفيّ أو شبي حرفيّ، أو حسابات تدّعي أنها لصحفيين، دون أن تتضمّن معلومات تفصيلية عن مكان العمل والسيرة المهنية، أو تتضمّن معلومات مفبركة.

كما يشمل ذلك المواقع الإلكترونية التي تسرق المحتوى من مواقع أخرى، ثم تدسّ بين المقالات المسروقة مقالات متحيّزة أو إشكالية أو مضللة. إضافة نطاق واسع من العوامل والسمات الأخرى.

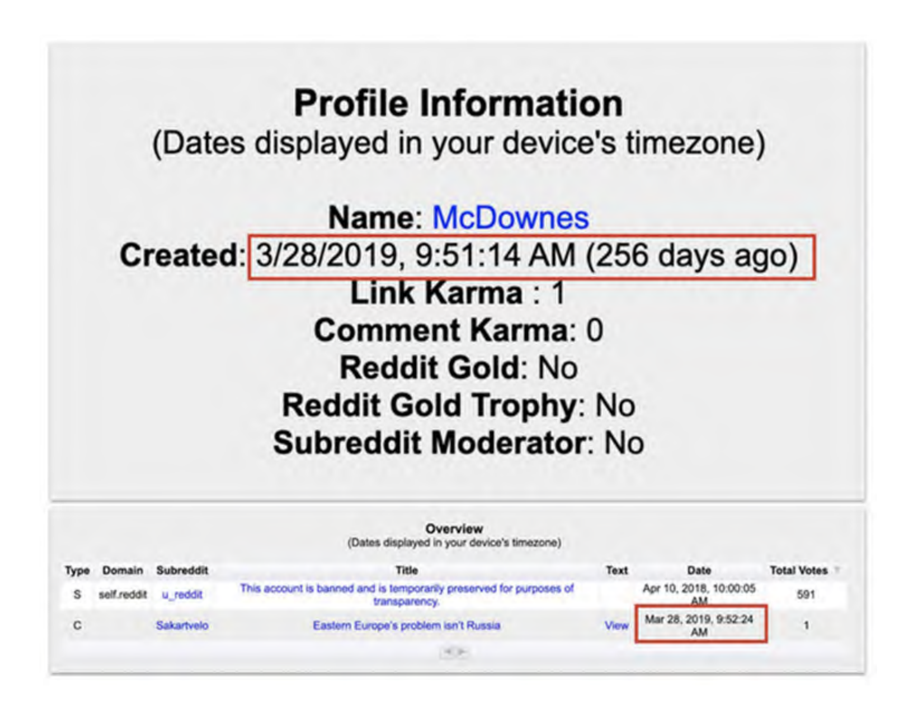
وما يتعيّن على الصحفي القيام به هو التحرّي عن السمات المثيرة للريبة وتحديد ما يلزمه من مختلف السمات وأنماط السلوك الرقمية الأخرى؛ بما يتيح له أن يتوصل إلى قناعة بأن هذا الحساب أو الموقع جزءٌ من عملية أكبر.



تحديد نمط في السلوك الرقمي: مقال نشر على موقع الخميني، ثم نشر دون نسبة إلى المصدر الأصلي على موقع IUVMpress.com وBritishleft.com، وهما موقعان ضمن شبكة لنشر البروباغندا الإيرانية. مصدر الصورة: DFRLab.

في أحيان أخرى يكون غياب مثل هذه السمات والأنماط من السلوك الرقمي مؤشرًا في حد ذاته على إشكال ما. وقد كانت تلك هي الحال

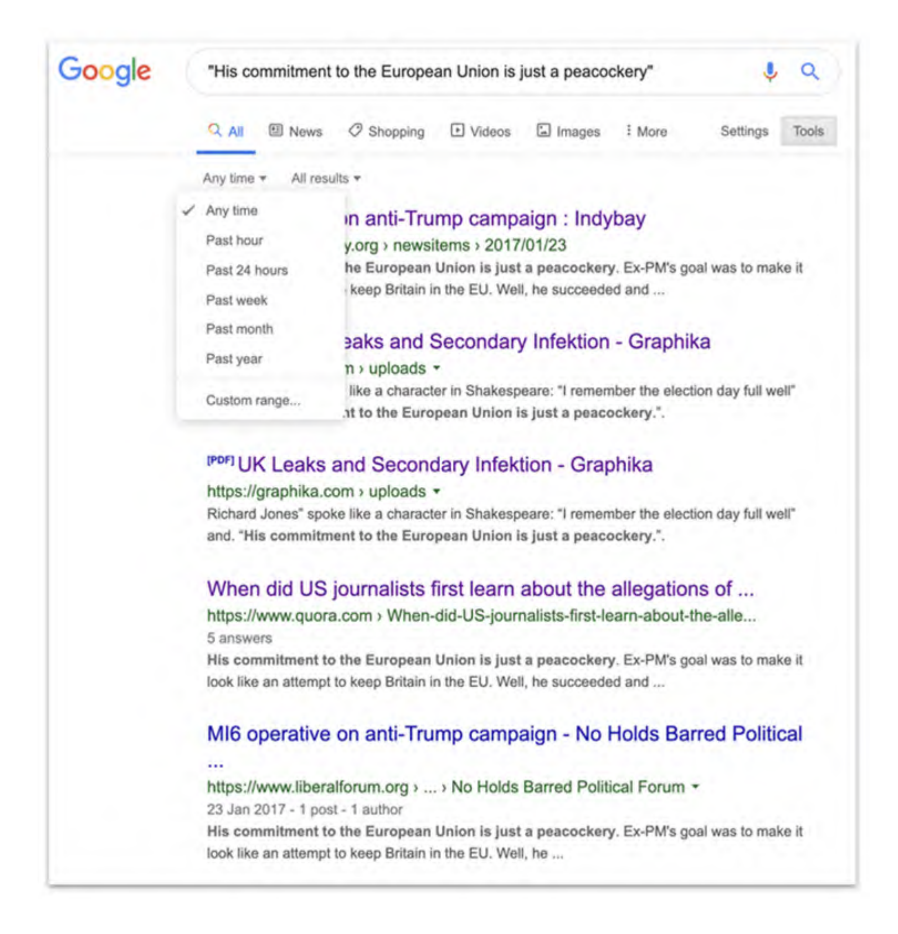
فـي عمليـة "Secondary Infektion" التـي كانـت تـدار مـن روسـيا، والتـي اسـتخدمت مئـات الحسـابات فـي عـدد مـن منصـات التدويـن، وجميعهـا كانـت تشـتمل علـى الحـدّ الأدنـى مـن النبـذ التعريفيـة الشـخصية، وجميعهـا أيضـا نشـر مقـالًا واحـدًا فـي اليـوم الـذي أنشـئت فيـه حسـاباتها، ثـم لـم يظهـر لهـا أي نشـاط بعـد ذلـك. وقد كان هـذا النمـط الأساسـي مـن السـلوك ثابتًـا لـدى عـدد كبيـر مـن الحسـابات، حتـى تبيّـن أثنـاء عمليـة التحقيـق أن هـذه هـي "البصمـة" التـي اعتمدهـا القائمـون علـى العمليـة. وعندمـا قامـت حسـابات مجهولـة فـي الترويـج لوثائـق تجاريـة سـرية بيـن المملكـة المتحـدة والولايـات المتحـدة الأمريكيـة قبيـل الانتخابـات العامـة فـي بريطانيا في ديسـمبر 2019، أظهـرت "غرافيـكا" ورويتـرز أن هـذه الحسـابات قـد اتبعـت نفـس هـذا السلوك، وهو ما أكّدته كذلك منصّة ريديت.



بروفايـل على ريديـت لحسـاب باسـم "McDownes" مرتبـط بحسـب ريديـت بعمليـة "Secondary Infektion". تـم إنشـاء الحسـاب في 28 مـارس 2019، ونشـر مقـالًا وحيـدًا في غضـون دقيقـة واحـدة بعـد إنشـائه، ثـم توقـف نشـاطه تمامًـا. الصـورة مـن "غرافيـكا"، والبيانـات مـن موقـع reductive.com.

يمكن الاستفادة من المحتوى كذلك لتمييز الحسابات أو المواقع التي قد تكون ناشطة ضمن شبكة واحدة. فلو لاحظت مثلًا أن الأصل الذي تتحرى عنه يشارك صورة أو مقطعًا معينًا، فمن الضروري البحث عن الصورة أو لقطة الشاشة بخاصية البحث العكسي لمعرفة ما إذا كانت قد نشرت في أماكن أخرى. يمكن الاستفادة من أداة RevEye التي يمكن إضافتها على محرك البحث، ولاسيما أنها تتيح للصحفيين البحث عن الصورة بشكل عكسي على جوجل، وياندكس، وتين آي، وبايدو، وبينغ. فمن المفيد دومًا البحث عبر محركات بحث مختلفة، وذلك لأنها قد تقدّم أحيانًا نتائج مختلفة.

وفي حال نُشر نص معين من قبل هذا الأصل المشبوه، فمن الضروري البحث عن المواضع الأخرى التي ظهر فيها النص نفسه. وفي حال كان النص طويلًا، فمن الأفضل البحث باستخدام جملة من الفقرة الثالثة أو الرابعة من النص أو ما بعدها، وذلك لأن الناشطين في مجال التضليل يلجؤون عادة إلى التعديل على العناوين والعناوين الفرعية، وربما الفقرة الأولى، ولكنهم يهملون تعديل ما تبقى. وعبر حصر الجمل التي تود البحث عنها بعلامات التنصيص "جملة البحث" فإنك ستحصل على نتائج توضّح المواضع الأخرى التي استخدمت بها هذه الجمل. ويمكن كذلك الاستفادة من قائمة "الأدوات" "tools" من أجل فلترة النتائج حسب التاريخ.



نتائج عملية بحث على جوجل عن جملة نشرت في حملة تضليل روسية محتملة، ويظهر كيفية استخدام الأدوات في محرك البحث لتصفية النتائج حسب التاريخ.

قد تكون هنالك كذلك أهمية للنظر في المنشورات التي تتضمن أخطاء إملائية، وذلك لأن الأخطاء بطبيعتها ليست هي الأصل.

فمثلًا، نلاحظ في مقال -نُشر ضمن عملية يتوقع أنها من تنظيم الاستخبارات الروسية- استخدامَ كلمة "Solsbury" للإشارة إلى مدينة "Salisbury"، وهي المدينة البريطانية حيث تعرض العميل الروسي السابق سيرجي سكريبال للتسميم. وقد أظهر البحث عن الكلمة بهذا

الرسم الإملائي الخاطئ نتائج محددة في محرك البحث، وهي نتائج قد تفيد بالتوصل إلى نتيجة ما بعد التحرّي عن سبب استخدام الكلمة بتهجئة خاطئة.

وبالإضافة إلى الاستفادة من المؤشرات والدلائل من المحتوى، فإنه من المهم البحث عن مؤشرات أخرى في أنماط السلوك الرقمي، للتأكد إن كان حساب أو موقع ما جزءًا من عملية واسعة. هنالك أسباب عديدة تدفع المستخدمين العاديين لنشر محتوى وصلَهم ضمن عملية تضليل ما، ما يعني أن مجرد تتبع عمليات نشر المحتوى ليس دليلًا قويًا بذاته على وجود عملية منسَّقة. فالعديد من الناس قد نشروا "ميمز" صممتها وكالة أبحاث الإنترنت الروسية، ولكن السبب هو أن هذه "الميمز" كانت ذات سمات تسمح لها بتحقيق ذلك القدر من الرواج.

جمع الأدلة

عمليات التضليل والتأثير معقدة وسريعة، وأشد ما في عمل الصحفي إحباطًا إذا كان يعتمد على المصادر المفتوحة هو أن تختفي مجموعة من الحسابات أو المواقع التي يتعلق التحقيق بنشاطها. لذلك فإن التصرف الأسلم في هذه الحالة هو توثيق كل ما تقع عليه بمجرد اكتشافه، وذلك لأنه قد لا تتاح لك فرصة أخرى لعرضه.

وتختلف تفضيلات الباحثين بشأن تسجيل الأصول التي يعثرون عليها؛ إذ تختلف المتطلبات من عملية إلى أخرى.

جداول البيانات مفيدة لتسجيل المعلومات الأساسية الخاصة بأعداد كبيرة من الأصول (المواقع الإلكترونية أو الحسابات)، أمّا الملفات المشتركة المخزنة في الخدمات السحابية فهي طريقة جيدة لتخزين أعداد كبيرة من لقطات الشاشة (screenshots)، ويفضّل بطبيعة الحال أن تحفظ كل لقطة شاشة باسم يدلّ على محتواها، وذلك لعدم تضييع الوقت لاحقًا

في محاولة البحث عن لقطة الشاشة التي تريدها من بين 100 أو أكثر من لقطات الشاشة التي جمعتها.

يمكن كذلك الاستفادة من ملفات الوثائق العادية (Text Documents) لتسجيل ما يلزم من معلومات، إلا أنها سرعان ما تصبح غير منظمة، خاصة إن كانت العملية كبيرة.

وأيًا كان الشكل الذي تختاره؛ فعليك أن تحرص بشكل خاص على تدوين بعض المعلومات الأساسية، والتي تشتمل أولًا على كيفية الوصول إلى الأصل موضوع التحقيق (الحساب أو الموقع)، وهذه نقطة أساسية يجب بيانها بوضوح، إضافة إلى الاسم والرابط، وتاريخ الإنشاء (إنْ توفّر)، وعدد المتابِعين، والمتابَعين، والإعجابات و/أو المشاهدات. كما يشمل ذلك وضع وصف مختصر للأصل (مثلا: حساب باللغة العربية يروج للسعودية وصورة البروفايل لإيما واتسون)، وذلك لتسهيل الرجوع إليه في حال تحريت عن 500 حساب آخر بعده. أما إن كنت تعمل مع فريق، فمن المهم تسجيل اسم الشخص الذي يكتشف أي أصل.

أما الروابط فيمكن حفظها باستخدام خدمات الأرشفة، مثل Wayback Machine أو Archive.is، لكن عليك أن تحرص على عدم كشف مستخدمين حقيقين ربما تفاعلوا بشكل عفوي مع الأصول المشبوهة التي تتحرى عنها، وتأكد كذلك أن الرابط المؤرشَف يحفظ المواد البصرية التي تظهر على الرابط الأصلي، ومن الأفضل أن تأخذ لقطات شاشة احتياطًا.

تأكد أيضًا من حفظ الأصول وما يتعلق بها بشكل آمن، كأن تضعها في ملفات محمية بكلمة مرور أو محافظ بيانات محميّة، وعليك أن تعرف من يستطيع الوصول إليها، وراجع باستمرار تاريخ الولوج إليها لو لزم.

وأخيرًا لا بدّ من تقديم تقييم بمستوى الثقة بأصل ما. فكثيرًا ما تجد حملات التأثير والتضليل مستخدمين عاديين يروجون لمحتواها بشكل

غير مقصود، وعادة ما يكون هذا هو الهدف من الحملة أصلًا، بأن تدفع الناس العاديين لتبنّي رأيٍ ما والترويج له. لذلك لا بد لك من وضع تقييم يوضّح مستوى اقتناعك بأن أصلًا ما هو جزء بالفعل من عملية أوسع، وتقديم السبب الذي يدفعك لتصديق ذلك.

ولا بدّ أن يكون تقييم الثقة من طرفك (عال، متوسط، ضعيف) واضحًا في جزء منفصل ضمن البيانات التي تسجلها عن الأصل الذي تتحرى عنه، إضافة إلى الأسباب التي تفسّر هذا التقييم.

تحديد الأطراف وتقييم الثقة

إنّ التحدي الأكبر فيما يتعلق بالحكم على عمليات التأثير والتضليل الموجّهة يكمن في نسبتها إلى طرف محدّد. ومن المهم التنبه هنا إلى أنه وفي العديد من الحالات يكون تحديد هذا الطرف بشكل قطعي أمرًا يقع خارج إمكانات الصحفي أو المحقق الذي يعتمد على المصادر المفتوحة. لذا فإن الوسيلة الأفضل لمقاربة هذا الأمر هي وضع تقييم تقريبيّ للثقة في أن جهة ما هي التي تقف وراء الحملة التي تم التحقيق بشأنها أو أن بعض الأصول التي تم التحري بشأنها لها علاقة بعملية محددة. أما تقديم حكم قاطع بخصوص الجهة التي تدير حملة ما فنادرًا ما يكون أمرًا ممكنا بمجرّد الاعتماد على المصادر المفتوحة.

بعض المعلومات الأساسية، مثل بيانات تسجيل اسم النطاق الخاص بموقع إلكتروني، أو عناوين بروتوكول الإنترنت، أو أرقام الهواتف، يمكن أن تساعد في تشكيل رأي يتعلق بنسبة حملة ما إلى جهة معينة، إلا أنها تبقى عادة معلومات محجوبة عن الجميع باستثناء منصات التواصل الاجتماعي. ولهذا السبب فإن التواصل مع المنصات جزء أساسي من العمل الاستقصائي. وبما أن منصات التواصل الاجتماعي قد عزّزت من عملياتها الداخلية عبر فرق استقصائية خاصة، فإنها باتت أكثر رغبة بالمساعدة في زيادة مستوى الشفافية العامة فيما يتعلق بالجهات التي يلاحَظ أنها تدير حملة ما.

لذا فإن الحالات التي تم فيها تأكيد نسبة حملة ما إلى جهة معينة، تضمنت تدخلًا مباشرًا من هذه المنصات، ومن أمثلة ذلك ما قامت به تويتر من الكشف عن عمليات تلاعب إعلامي مدعومة من جهات رسمية صينية تستهدف هونغ كونغ، وما قامت به فيسبوك من الكشف عن عمليات لها ارتباط بالحكومة السعودية.

كما أنّ المحتوى نفسه له دور يساعد في الكشف عن الحملات والجهات التي تديرها؛ مثل ما حدث عند الكشف عن عملية على إنستغرام في أكتوبر 2019 قامت بنشر "ميمات" متماثلة تقريبًا مع ميمات أخرى نشرتها وكالة أبحاث الإنترنت الروسية، ولكنها لا تحمل توقيعها (العلامة المائية الخاصة بالوكالة). لقد كانت الطريقة الوحيدة الممكنة لتصميم هذه الميمات هي البحث عن الصور الأصلية التي استخدمت في ميمات الوكالة، ثم تصميم الميمات بالاعتماد عليها. وللمفارقة، فإن هذه المحاولة لمعرفة أصل المنشورات الخاصة بالوكالة قد أدت إلى الكشف عن أن من صمم هذه الميمات هي بالفعل الوكالة نفسها.

وقد حصل أيضًا قيام شبكة كبيرة من مواقع إلكترونية، يبدو ظاهريًا أنها غير مرتبطة بشبكة واحدة، بنشر مقالات منسوخة عن مصادر حكومية إيرانية، من دون نسبة المقالات إلى مصدرها. وقد تكرر هذا النمط من السلوك في هذه المواقع، حتى تبين أن هذا هو نشاطها الرئيسي، والذي نُسب في النهاية لأطراف ذات أجندات داعمة لإيران، لكنه لم يكن كافيًا للجزم بأنه نشاط تقوم به أطراف تابعة للحكومة الإيرانية نفسها.

ما يلزم التأكيد عليه هنا هو أن نسبة حملةٍ إلى جهة يتطلب الكثير من الانضباط وعدم التسرع، ولا بدّ أن يسبق إطلاق الحكم على الجهة المسؤولة عن حملة ما التأكد بشكل واضح من القدرة على إجابة السؤال المشروع: "كيف لك أن تثبت اتهامك لهذه الجهة بأنها هي التي تدير هذه الحملة؟". فإن لم يكن الجواب واضحًا على هذا السؤال، فلا بدّ من الإحجام عن إلقاء الاتهامات. إن الكشف عن

حملات التلاعب والتضليل وتحديد الأطراف الذين يقفون وراءها هو جهد بالغ الصعوبة والتعقيد، وإلقاء اتهام لجهة ما دون امتلاك دليل قطعي على ذلك من شأنه أن يقوّض كل الجهود السابقة التي قمت بها حتى تلك اللحظة.

دراسة حالة 1: من كان يقف وراء عملية "Endless Mayfly"

غابرييل ليم

غابرييل ليم: باحثة في مشروع أبحاث التكنولوجيا والتغير الاجتماعي في مركز شورنستين التابع لكلية كينيدي في جامعة هارفارد، وحاصلة على زمالة مؤسسة "سيتيزن لاب" (Citizen Lab). تهتم غابرييل بدراسة تأثير الرقابة والتحكم بوسائل الإعلام على الأمن وحقوق الإنسان.

في أبريل 2017، تم رصد مقالٍ مفبرك نشر على ريديت ويدّعي أنه ظهر من الإندبندنت البريطانية.

المقال يكذب على لسان نائب رئيسة الوزراء السابقة، نيك كليغ، ويقول: إن رئيسة الوزراء السابقة تيريزا ماي كانت "تتزلّف للأنظمة العربية". بعض مرتادي المنصّة الحريصين تنبهوا إلى ذلك المنشور وأوضحوا أنّه مريب ومفبرك. فالمقال ظهر على موقع indepnedent.co وليس على www.independent.co.uk، كما كان المنشور الأصلي يحاكي الموقع الأصلي في تصميمه، وقد نشر عدة مقالات مفبركة أخرى على ريديت.

هذه الحالة التي تضمنت فبركة مقال وموقع إلكتروني وشخصية وهمية أثارت اهتمام الباحثين في "سيتيزن لاب"، ودفعتهم لقضاء 22 شهرًا في التعقب والتحري عن الشبكة التي وقفت وراء تلك الحملة الرقمية المضللة، والتي حملت اسم "Endless Mayfly". وقد كان الهدف من هذه الحملة استهداف الصحفيين والناشطين عبر مواقع زائفة تحاكي مواقع حقيقية، ونشر معلومات كاذبة ومضللة عبرها.

كان الأسلوب الذي اتبعته الحملة عمومًا هو تقليد مواقع إخبارية محترمة ونشر مقالات مفبركة والترويج لها عبر شبكة من المواقع الإلكترونية والحسابات المزيفة على تويتر، ثم حذف المقال أو إعادة توجيهه بمجرد أن يتصاعد الزخم الرقمي بشأنه. فيما يلي مثال على مقال مفبرك يدّعي أنه من Bloomberg، ولكنه يتلاعب على القارئ عبر استخدام تهجئة خاطئة لاسم الوكالة الإعلامية، فيكتبها Bloomberq.com:

Bloomberg the Company & its Products | Bloomberg Anywhere Remote Login | Bloomberg Terminal Demo Request

Former CIA Director: Giving CIA Medal of Honor to Saudi Crown Prince Clever Move to Support Him Against Nephew

by Billy House
March 10, 2017, 10:01 PM GMT Updated on March 11, 2017, 12:01 AM GMT

- House Intelligence panel sets first public hearing March 20
- Committee invited NSA's Rogers, Brennan, Clapper, Yates



BloombergPolitics | Former CIA Director: Giving CIA Medal of Honor to Saudi Crown Prince Clever Move to Support Him Against Nephew

John Brennan in Fairfax, VA, on March 10, 2017. Photographer: Elise Amendola/AP

Former CIA Director John Brennan told Bloomberg reporter that he supports Pompeo's travel to Middle East specially Turkey and Saudi Arabia and assesses it as a fruitful trip adding: "giving the CIA Medal of Honor to Saudi Crown Prince, Mohammad bin Naif was a clever move by Washington to support him against his younger Nephew, Muhammad bin Salman."

"It seems Trump gave Middle East case to the CIA and there is traditional coordination between CIA senior officers and Mohammad bin Naif," Brennan added.

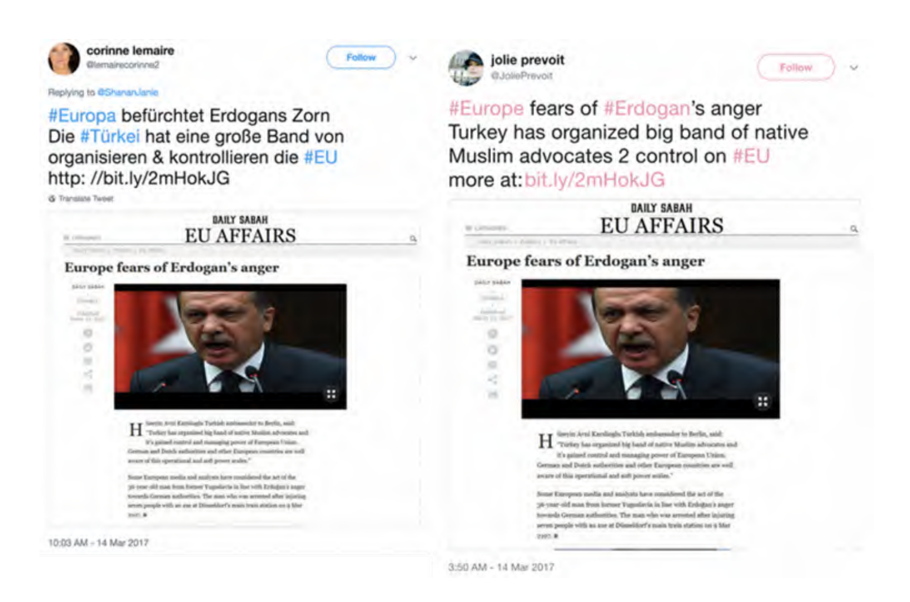
America's foreign policies in Middle East led to Pompeo's trip to Turkey and Saudi Arabia, and following it Adel Al-Jubeir's travel to Turkey and Iraq that shows CIA's plan for future of Middle East. Adel Al-Jubeir is one important CIA puppet among Saudi authorities.

Keep up with the best of Bloomberg Politics.
Get our newsletter daily.
Enter your email | Sign Up

Most Read

- Trump's Clash With Justice Department Sparks `You're Fired'
- Trump Points to Drudge's 'Great Again' Praise of New Jobs Report
- Merkel to Warn Trump That U.S. Tax Changes May Spark Retaliation
- U.S. Jobs, Pay Show Solid Gains in Trump's First Full Month
- Donald Trump Has Call Centers in the Philippines Worried

يظهر في الصورة أدناه شخصيتان وهميتان مرتبطتان بعملية Endless Mayfly، ينشران تغريدة برابط لمقال يدّعي أنه من "ديلي صباح" التركية على نسخة مقلّدة من الموقع. لاحظ أن الحساب باسم "Jolies Prevoit" يستخدم صورة للممثلة إليشا كوثبيرت كصورة للبروفايل.



وفي وقت نشر تقريرنا في مايو 2019، كان لدينا قاعدة بيانات تشتمل على 135 مقالًا، و72 موقعًا إلكترونيا، و11 شخصية وهمية، ومؤسسة وهمية، وشبكة نشر داعمة لإيران تعمل على ترويج المعلومات الزائفة التي تضمنتها المقالات المفبركة. وقد خلصنا في النهاية بمستوى معقول من الثقة بأن عملية "Endless Mayfly" كانت عملية تضليل إعلامية تخدم مصالح إيرانية.

يوضّح هذا المثال كيفية الجمع بين عمليات تحليل الشبكة والمحتوى والاستفادة من المصادر الخارجية من أجل الوصول إلى حكم ينسب عمليّة ما إلى جهة محددة. كما يوضّح المثال الصعوبة التي تحيط بالجهود الرامية إلى معرفة الطرف الذي يقف وراء عملية تضليل واسعة، والسبب الذي يستدعي البحث عن قدر كاف من الأدلة والمؤشرات، وكيفية استخدام مستوى الثقة لبيان الحكم الذي توصّل إليه التحقيق في نسبة العملية إلى الطرف المشتبه به.

ولا بدّ من التأكيد مجددًا على صعوبة الحكم بارتباط طرف ما بعملية تضليل على الشبكة، وسبب ذلك عادة هو المعلومات غير المكتملة، دون أن يكون لديك اعتراف من طرف معيّن أو دليلٌ قاطع على حكمك. وهذا ما يجعل الحكم في مثل هذه الحالات يقدّم باستخدام تقديرات ترجيحية بناء على المعلومات التي تمكّن الصحفي من الوصول إليها.

حصر نقاط البيانات وعمليات التحليل

نظرًا للطبيعة السريّة لعمليات التضليل والتلاعب الإعلامي، وطبيعة الأدلة الرقمية وإمكانية إخفائها، ونظرًا لقدرة الأطراف الفاعلة في هذه العمليات على الانخراط في أنشطة "تمويه" أخرى تلفت النظر عن العملية الأساسية، فإن الجهود التي تحاول الكشف عن الشبكة ومعرفة الجهة التي تقف وراءها لا بدّ أن تعتمد على توليفة من عمليات التحليل وجمع الأدلة.

في حالة "Endless Mayfly" توصلنا بقدر معقول من الثقة إلى أنها كانت عملية مرتبطة بأطراف داعمة لإيران، وذلك بالاعتماد على مؤشرات تم جمعها عبر ثلاثة أنواع من التحليل:

1. تحليل المحتوى
2. تحليل الشبكة
3. المصادر والتحليلات الرديفة

1. تحليل المحتوى

بعد عمليات تحليل المحتوى والخطاب في 135 مقالاً مفبركًا جمعناها في هذا التحقيق، توصلنا بشكل واضح إلى أن السرديّة التي تسعى المقالات إلى ترويجها هي سردية داعمة للمصالح الإيرانية. وقد صنفنا كل واحد من المقالات في فئة من الفئات التي حددناها بعد الاطلاع على كافة المقالات من أجل تصنيفها. وقد تم تصنيف المقالات على مرحلتين:

المرحلة الأولى جرت بشكل منفصل من قبل باحثين اثنين، أما المرحلة الثانية فكانت مشتركة من قبل فريق البحث بالإضافة إلى الباحثَين في المرحلة الأولى، وذلك للتأكّد من عدم وجود أي تباين في الآراء حول التصنيف. ويوضح الجدول الآتي نتائج عمليات التصنيف التي أجريناها:

Category	Article count	Category description
Geopolitical discord	63 (46.7%)	The article describes events, actions or statements made by government officials toward a foreign state that may be construed as provocative, hostile or counter to the foreign state's interests.
Domestic discord	16 (11.9%)	The article describes events, actions or statements made by political actors that may sow discord between political parties or actors within the same state.
Cooperating with Israel	14 (10.4%)	The article describes events, actions or statements made by political actors or government officials that show cooperation between Israel and another state.
Saudi Arabia supports terrorism	9 (6.7%)	The article describes events, actions or statements that either link Saudi Arabia to terrorist activity or allege that Saudi Arabia supports terrorism.
Other	5 (3.7%)	The article does not fit into any of the categories.
No archive	31 (23%)	The article cannot be coded because it no longer exists and there is no cache, screenshot or copy of the text to perform any meaningful analysis.
Copy of existing article	5 (3.7%)	The article is a direct copy/paste of an already existing real article.

وبعد تصنيف كافة المقالات، حددنا بشكل واضح السرديات المشتركة التي حاولت المقالات ترويجها في عملية Endless Mayfly. ثم عمدنا إلى مقارنة هذه السرديات بما يتوفر لدينا من أبحاث أولية عن المنطقة المستهدفة، وقد تطلب ذلك إجراء أبحاث مكثفة لفهم طبيعة الاستقطاب والتحالفات في المنطقة، والمصالح والتهديدات الجيوإستراتيجية، مع خلفية تاريخية عن عمليات التضليل والتلاعب الإعلامي السابقة.

وكان هدف هذه الخطوة المساعدة في وضع الأدلة والمؤشرات في سياقها وفهم السرديّات التي حاولت المقالات الترويج لها في سياقها السياسي الأوسع. وبالنظر إلى المقالات التي جمعناها والسرديات التي تخدمها

بحسب التصنيف الذي وضعناه، فإننا توصلنا إلى رأي يرجّح أن تكون هذه المقالات ضمن عملية تخدم مصالح إيرانية.

2. تحليل الشبكة

أجرينا عمليات تحليل الشبكة من أجل تحديد المنصات وأسماء النطاقات التي ساهمت في الترويج للمحتوى. وفي عملية Endless Mayfly تم تحديد شبكتين انخرطتا بشكل أساسي في نشر المقالات المفبركة والمعلومات الزائفة التي تضمنتها: الأولى شبكة من مواقع إلكترونية داعمة لإيران، والثانية شبكة من الحسابات الوهمية على تويتر. وقد بدا أن كلتا الشبكتين مرتبطةٌ بالعملية، وذلك لأنهما نشطتا بالترويج للمقالات المتسقة مع السياسات الإيرانية الرسمية، والبيانات الرسمية للحكومة الإيرانية ومواقفها من السعودية وإسرائيل والولايات المتحدة.

شبكة النشر

تتألف شبكة النشر في هذه العملية من عدد من المواقع التي يظهر أنها موالية لإيران، رغم أنها تدّعي أنها مواقع إخبارية مستقلة. وكان مجموع ما أحصيناه ووثقناه هو 352 صفحة ويب عبر 132 اسم نطاق نشرت أو وضعت روابط للمقالات المفبركة المرتبطة بعملية Endless Mayfly.

وقد أجرينا هذه العملية عبر البحث في جوجل عن روابط المقالات المفبركة موضوع التحقيق وعناوينها. كما تفحصنا الروابط التي نشرتها الحسابات الوهمية على تويتر، كي نصل إلى صفحات الويب التي نشرت المقالات أو اشتملت على روابط تنقل إليها.

وعبر هذه العملية تمكنا من تحديد أهم 10 مواقع كانت تنشط في نشر المقالات المفبركة. ومن بين هذه المواقع العشرة اكتشفنا أن ثمانية منها تشترك في عنوان بروتوكول الإنترنت أو بيانات تسجيل اسم النطاق، ما يدلّ على أنها قد تكون تابعة لجهة واحدة.

أما محتوى هذه المواقع فكان في معظمه يروّج لوجهة نظر ومصالح إيرانية. فموقع IUVM Press، والذي نشر أو تضمن روابط للمقالات المفبركة في

عمليـة Endless Mayfly 57 مـرة، تضمـن وثيقـة PDF بعنـوان "الميثـاق" والتــي تشـير بوضـوح إلــى أن الموقع مناهض لأنشـطة ومشـاريع "قوى الغطرسـة والإمبرياليـة والصهيونيـة"، وتقـول بوضـوح إن "المقـر الرئيسـي للاتحـاد يقـع في طهران، عاصمة الجمهورية الإسلامية الإيرانية".

شبكة الحسابات الوهمية

كانـت شـبكة الحسـابات الوهميـة علـى تويتـر والمرتبطـة بعمليـة Endless Mayfly تنشـر محتـوى شـديد النقـد لسياسـات السـعودية وإسـرائيل والـدول الغربيـة عمومًـا، بشـكل متسـق مـع محتـوى المقـالات المفبركـة والمواقـع الإلكترونية موضوع التحقيق.

وعبـر عمليـة تحليـل لنشـاط هـذه الحسـابات علـى تويتـر تبيـن لنـا أنهـا حسـابات تنشـط فـي نشـر روابـط لمقـالات مفبركـة وأخـرى حقيقيـة تشـتمل علـى انتقـادات شـديدة لخصـوم إيـران السياسـيين. مـن بيـن هـذه الحسـابات مثـلًا حسـاب يدعـي أنـه يمثـل مؤسسـة (Peace, Security, Justice Community)، وهـي مؤسسـة وهميـة بحسـب مـا يظهـر أدنـاه، ينشـر بشـكل أساسـي محتـوى مناهـض للسـعودية وإسـرائيل والولايـات المتحـدة، كمـا أنـه يسـتخدم صـورة بروفايـل ونبـذة تعريـف تعبـر عـن عـداء واضـح للسعودية، تقول: إن الأيديولوجية الوهابية للسعودية هي مصدر التطرّف.



وفـي حسـاب وهمـي آخـر ضمـن هـذه الشـبكة باسـم (Mona A. Rah-man)، نجـد ذكـرًا لشـخصية سـعودية معارضـة وهـو علـي الأحمـد، فـي الوقـت الـذي تنتقـد فيـه ولـيَّ العهـد السـعودي محمـد بـن سـلمان وتصفـه بـ "المجرم البربري".



I invite the dissidents to gather against the murderous and barbarous Saudi crown prince next month in #London. My special thanks to Mr. Al Ahmed (@AliAlAhmed_en) who is strongly supporting this gathering. #JusticeforJamal #TrialforMBS #FreedomIsNear

11:30 PM - 17 Nov 2018



3. المصادر والتحليلات الرديفة

حرصنـا بالإضافـة إلـى العمليـات السـابقة علـى مقارنـة النتائـج التـي توصلنـا إليهـا مـع تحليـلات خارجيـة رديفـة. فبعـد معلومـة تـم الحصـول عليهـا مـن FireEye فـي أغسـطس 2018، عطلـت فيسـبوك بعـض الحسـابات والصفحات المرتبطة بشبكة النشر في عملية Endless Mayfly.

وقـد حـددت شـركة FireEye عـددًا مـن المواقـع الإلكترونيـة التـي كانـت جـزءًا مـن شـبكة النشـر التـي كشـفنا عنهـا، ومـن بينهـا موقـع -instituto manquehue.org وموقع RPFront.com وغيرها.

وبشـكل متسـق مـع مـا توصلنـا إليـه نحـن، فقـد توصـل تحقيـق الشـركة بقـدر معقـول مـن الثقـة إلـى أن العمليـةَ موضـعَ التحقيـق مصدرُهـا علـى الأرجـح

إيران. كما أشارت فيسبوك كذلك في بيانها إلى أن الحسابات والصفحات التي عطلتها كانت على الأرجح إيرانية.

إضافة إلى ذلك، كشفت تويتر عن قائمة من حسابات مرتبطة بإيران قامت المنصة بتعطيلها لتورّطها في أنشطة "تلاعُب منسقة". ومع أن تويتر لم تكشف عن أسماء الحسابات التي كان يقل عدد متابعيها عن 5000 متابع عند تعطيلها، إلا أننا تمكّنّا من معرفة أن أحدها كان جزءًا من عملية Endless Mayfly وهو حساب (@shammari_Tariq).

وقد ساعدتنا هذه العمليات التي قامت بها تويتر وفيسبوك وشركة "فاير آي"؛ إذ دعمت النظرية التي حاولنا إثباتها وقدمت أدلة إضافية لم تتوفر لدينا، وتقاطعت مع الأصول التي حددناها في عملية Endless Mayfly. ففي تحليل شركة "فاير آي" تم الوصول إلى أرقام هواتف ومعلومات تسجيل مرتبطة بحسابات تويتر ومواقع إلكترونية مرتبطة بعملية Endless Mayfly، وهي أدلة لم تشتمل عليها قاعدة البيانات التي جمعناها أثناء التحقيق.

كما كان لدى فيسبوك وتويتر معلومات خاصة بتسجيل الحسابات المشبوهة، مثل عناوين بروتوكول الإنترنت، وهي معلومات لم يكن بوسعنا التوصل إليها. وقد ساعدتنا هذه المعلومات الإضافية من أطراف خارجية بشكل كبير على توسيع حجم الأدلة التي لدينا لتعزيز ثقتنا بالنتيجة التي سعينا للتوصل إليها.

التوصل للحكم النهائي

في حالة عملية Endless Mayfly، كانت جميع الأدلة التي جمعناها - بما في ذلك المحتوى المتضمن لسرديات داعمة لإيران، وشبكة المواقع الإلكترونية والشخصيات الوهمية - تشير إلى أن إيران هي الطرف الذي يقف على الأرجح وراء تلك العملية.

ثم قارنّا ما توفر بين أيدينا من أدلة مع الأدلة الرديفة في عمليات تحقُّق قامت بها أطراف أخرى، مثل شركة "فاير آي"، وفيسبوك، وتويتر،

والتي عزّزت أيضًا من النتائج التي توصلنا إليها. فكل واحد من تلك الأدلة -رغم أنّه ليس كافيًا في ذاته للتوصل إلى حكم بشأن الجهة المسؤولة عن العملية- ساعد ضمن موقعه من الأدلة الأخرى التي جمعناها خلال التحقيق، في تأكيد ودعم نظريتنا. لكن ورغم المؤشرات العديدة التي كانت تدلّ على أيادٍ إيرانية في العملية، إلا أننا لم نمتلك الدليل القطعي الجازم على ذلك.

وهذا ما دفعنا إلى الاعتماد على إطار معتمد في مجتمع التحقيقات الاستخبارية ونسبة العمليات السيبرانية إلى جهات محددة، وهو إطار يستخدم أحكامًا ترجيحية حسب مستوى ثقة المحقق والمؤشرات المتوفرة لديه، بحيث يتمّ تقديم حكمٍ بمستوى الثقة (منخفض، متوسط، عال)، ما يتيح للمحققين إصدار نتائج لعمليات التحقيق المكثفة التي أجرَوها مع الإبقاء على نوع من التحفُّظ بحسب مستوى الثقة في الأدلة وكفايتها.

وقد توصلنا في نهاية المطاف وبمستوى "متوسط" من الثقة إلى أن عملية Endless Mayfly هي عملية داعمة لإيران.

وبحسب تعريف مكتب مدير الاستخبارات الوطنية الأمريكية، فإن هذا المستوى من الثقة يعني أن "المعلومات دقيقة وتم جمعها حسب الأصول، ولكنها غير كافية في ذاتها ولا يوجد ما يعزّزها بشكل كاف للوصول إلى مستوى أعلى من الثقة".

وقد فضّلنا أن نعبر عن ثقتنا "المتوسطة" بالحكم الذي توصلنا إليه؛ انطلاقًا من قناعة تشكلت لدينا بأن الأدلة التي جمعناها ليست كافية لاستبعاد احتمال أنها عمليةٌ "وهمية"، بمعنى أن تكون عملية يحاول طرف آخر أن يجعلها تبدو وكأن إيران هي المسؤولة عنها، أو احتمال أن من يقف وراء العملية هو طرف ثالث آخر قد يكون مجرّد متعاطف متحمّس للدفاع عن المصالح الإيرانية.

مثل هذه المحاولات للتوصل إلى الجهة المسؤولة عن عملية تلاعب أو

تضليل إعلامي، مثل عملية Endless Mayfly ستعتمد في كثير من الأحيان على معلومات ناقصة وستعتريها بعض الفجوات. لذلك فإن الاعتماد على مستويات الثقة بالأدلة والمؤشرات هي طريقة ملائمة للتعبير عن النتيجة المتعلقة بنسبة العملية لطرف ما، وذلك لأنها تحافظ على عنصر "التحفّظ" وعدم الجزم المطلق بالنتيجة سلبًا أو إيجابًا.

فليس ثمّة أخطر من إصدار حكم خاطئ بمسؤولية طرف ما عن إحدى العمليات، أو المبالغة بمقدار الثقة في نسبتها إلى جهة معينة، إذ يمكن لذلك أن يقوّض كل الجهود المبذولة في الكشف عن الشبكة وعملياتها، إضافة إلى احتمال أن يؤدي ذلك إلى عمليات أو إجراءات انتقامية تستهدف الصحفيين أو المؤسسات التي يعملون بها، خاصة لو كان الطرف المتّهم -دون أدلة كافية- هو جهة حكومية.

ولتجنب التسرع في إصدار الأحكام دون امتلاك ما يكفي من الأدلة، فإنه من الضروري مراجعة المؤشرات والأدلة وأنواعها وإجراء المزيد من التحليلات والتأكد من صحتها، والاستفادة من إطار مستويات الثقة لاستكشاف ما إذا كان يمكن وجود احتمالات أخرى أو بيانات ناقصة.

دراسة حالة 2: عملية تلاعب إعلامي في بابوا الغربية

بنيامين ستريك، إليس توماس

بنيامين ستريك: محقق يعمل لصالح بي بي سي، ويعتمد في تحقيقاته على المصادر المفتوحة، ويساهم أيضًا مع مؤسسة "Bellingcat" المتخصصة بالتحقيقات الرقمية. يقدم ستريك دورات تدريبية في استخدام تقنيات المصادر المفتوحة، والتحقيقات الجيومكانية وتحليل الشبكات، وله خبرة في المجالين القانوني والعسكري، وهو يركّز حاليًا على استخدام الأساليب المتبعة في "تحقيقات المصادر المفتوحة" و"التحقيقات الجيومكانية"، وذلك لغايات خدمة حقوق الإنسان وحل النزاعات وحماية الخصوصية.

إليس توماس: صحفية وباحثة مستقلة تعمل مع المركز الدولي للسياسات السيبرانية في المعهد الأسترالي للسياسات الإستراتيجية. وتكتب أليس مع العديد من الصحف والمجلات والمواقع، مثل موقع Wired، ومجلة فورين بوليسي، وموقع ديلي بيست، وصحيفة الغارديان وغيرها. وقد عملت سابقًا محررًا مساعدًا في مكتب الأمم المتحدة لتنسيق الشؤون الإنسانية، كما عملت في مجال الأبحاث وكتابة برامج البودكاست.

في أغسطس 2019 اندلعت أعمال عنف انفصالية في مقاطعة بابوا الغربية، والتي تم ضمّها لتكون جزءًا من إندونيسيا في خطوة مثيرة للجدل في ستينات القرن الماضي. وما تزال تشهد هذه المقاطعة حتى اليوم العديد من الحوادث التي تُتّهم فيها السلطات الأندونيسية بارتكابها انتهاكات حقوقية ضدّ السكّان المحليين الساعين للانفصال.

يعد الوصول إلى تلك المقاطعة مغامرة صعبة، وعادة ما يمنع الصحفيين الأجانب من دخولها وكتابة التقارير عنها. وفي مثل هذه الظروف فإن وسائل التواصل الاجتماعي تصبح الوسيلة المثلى لمعرفة ما يجري داخل المقاطعة وجمع المعلومات لإعداد التقارير الصحفية.

وأثناء محاولة لتحديد مكان بعض الصور ومقاطع الفيديو التي توثق أعمال عنف وقعت في منطقة "فاكفاك" في المقاطعة، لاحظ أحد الزملاء انتشار وسمين على تويتر، عما #WestPapua و#FreeWestPapua.

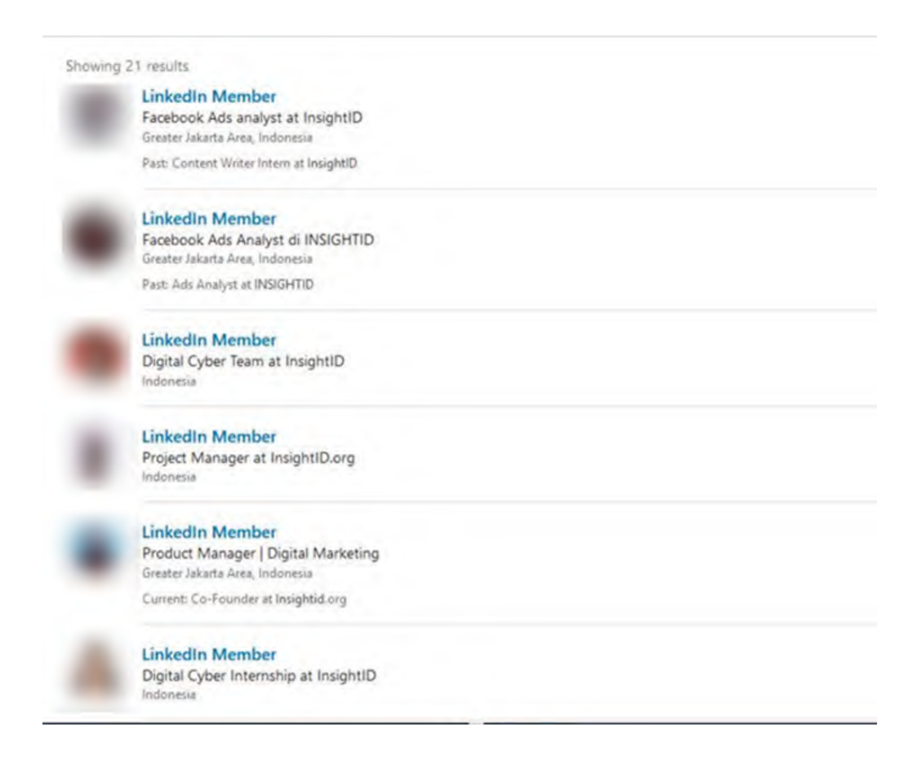
وقد كشف البحث عن المنشورات التي تضمنتها هذه الوسوم عن عدد كبير من الحسابات الوهمية التي تنشر بشكل آلي ومكثف نفس مقاطع الفيديو ونفس العبارات مع استخدام الوسمين أعلاه. كما نشطت هذه الحسابات في إعادة تغريد المحتوى فيما بينها والإعجاب بما ينشر عليها، في جهد واضح لترويج المحتوى وزيادة مستوى التفاعل مع الوسوم وتصعيدها.

وقد أوضحْنا في الفصل الثالث العمليات التي يجب اتباعها للكشف عن مثل هذه الحسابات وتحليل نشاطها. وبالاعتماد على تلك العمليات، توسعنا في التحقيق محاولين أن نحدّد الأشخاص أو الجهات التي تقف وراء هذه الحسابات. وحين بدأنا العمل على ذلك، اكتشفنا حملة أخرى مشابهة ولكنها أضيق نطاقًا، وغير مرتبطة -على ما يبدو- بالحملة الأولى التي اضطلعنا بمهمة التحقيق بشأنها، وقد تمكنّا من الكشف عن الشخص الذي يديرها، وهو أيضًا ما نجحنا في تحقيقه مع المسؤولين عن الحملة الأولى الأكبر، والذين اعترفوا كذلك بمسؤوليتهم عن الحسابات المفبركة، بعد أن تواصلت معهم بي بي سي.

لقد منحتنا الحملة الأولى بالنظر إلى حجمها ونشاطها على أكثر من منصة فرصة أوسع للبحث عن الأدلة والمؤشرات التي يمكن استخدامها للتوصّل إلى الأشخاص الذين يديرونها ومعرفة المزيد عنهم.

وأول ما أفادنا في هذا السياق هو المواقع الإلكترونية التي كانت الحسابات المشبوهة تنشر روابطها على تويتر وفيسبوك. فقد كشف لنا البحث عن بيانات تسجيل هذه المواقع أن أربعة منها مسجلة باسم وهمي وعنوان بريد إلكتروني عشوائي، ولكن مع رقم هاتف حقيقي.

بحثنا عن الرقم في تطبيق واتس آب ووجدنا أنه مرتبط بحساب لأحد الأشخاص، ويظهر في الحساب أيضًا صورة بروفايل يبدو أنها لصاحب الحساب. بحثنا عن الصورة في يانديكس، فظهر أنها كذلك مستخدمة على حساب في فيسبوك، ولينكد إن، وموقع Freelancer.com. وعبر الاطلاع على الحساب الذي توصلنا إليه في لينكد إن، تبين لنا أيضًا الجهة التي يعمل بها صاحب الحساب، كما اطّلعنا على قائمة زملائه.



لقد كان الشخص الذي حددناه موظفًا في شركة مقرها في جاكرتا واسمها InsightID، وهي شركة تصف نفسها في موقعها الرسمي بأنها شركة "لحملات العلاقات العامة والتسويق الرقمي".

وقد جمعنا كذلك بيانات إضافية تدلّ على أن هذه الشركة كانت المسؤولة عن العملية المشبوهة على تويتر. فالشركة تذكر على موقعها أنها تعمل على مبادرة بعنوان "مبادرة برنامج التنمية في بابوا"، وهي مبادرة بحسب ما ورد في الموقع "تعنى بدراسة التطورات الاجتماعية والاقتصادية في بابوا الغربية وتحديد التحديات التي تواجه المقاطعة". وقد وصف موظفون ومتدربون سابقون في الشركة عملهم على إنتاج مقاطع فيديو وكتابة وترجمة محتوى خاص بمبادرة التنمية في بابوا.

وقد ذكر أحد الموظفين السابقين على حسابه في لينكد إن أن الأعمال التابعة للمبادرة تعرض على موقع "West Papuan" وحساباته على فيسبوك وإنستغرام، وهو واحد من خمسة مواقع إخبارية ضمن الحملة. موظف آخر في شركة InsightID أنشأ حسابًا على يوتيوب باسم الشركة لرفع مقطع فيديو كان جزءًا من الحملة، ثم ضمّن الفيديو لاحقًا على موقع westpapuan.org.

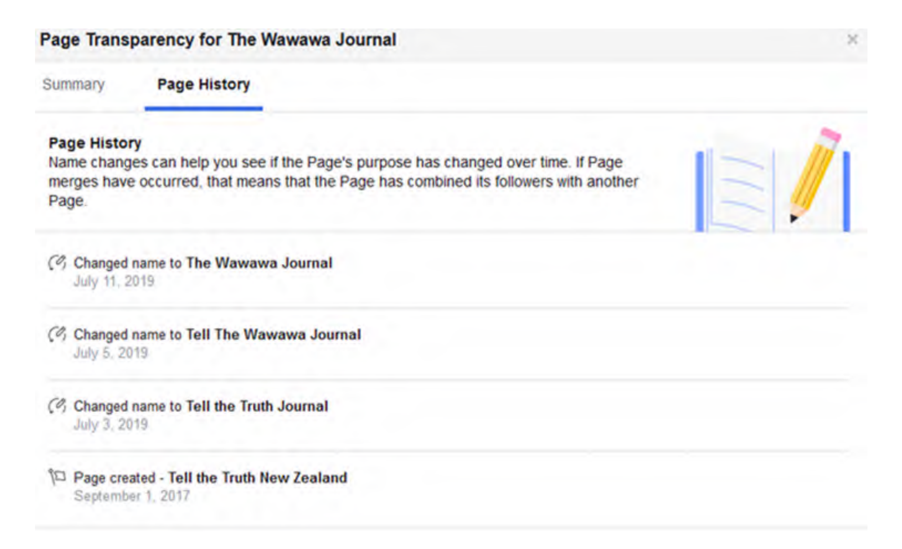
وقد كشفت عمليات البحث عن اسم النطاق أن المؤسس الشريك لشركة InsightID قد استخدم عنوانه البريدي المهني التابع للشركة لتسجيل 14 اسم نطاق في اليوم ذاته، وجميعها كانت مرتبطة بشكل واضح بمقاطعة بابوا الغربية، وكان من بينها مثلًا موقع westpapuafreedom.com، وwestpapuagenocide.com، وwestpapuafact.com وغيرها. وكل دليل إضافي جمعناه كان يصبّ باتجاه تأكيد تورّط شركة InsightID في العملية.

بعدها قرر صحفيون يعملون مع بي بي سي التواصل مع الشركة لطلب التعليق من طرفها، لكن الشركة أحجمت عن التعليق على الموضوع في البداية، ثم اضطرت لاحقًا للاعتراف عن مسؤوليتها عن العملية، وذكرت في منشور على وسائل التواصل الاجتماعي أن "المحتوى الذي ننشره يدافع عن المصالح الوطنية ضدّ المعلومات الزائفة التي تنشرها المجموعات الانفصالية في بابوا الغربية". لكننا في المقابل لم نتمكن من معرفة الطرف الذي استعان بخدمات InsightID للقيام بتلك الحملة.

وقد اكتشفنا أثناء التحقيق في هذه العملية شبكة أخرى أصغر تتألف من ثلاثة مواقع إلكترونية تدعي أنها مواقع إخبارية مستقلة، وكان لها حسابات على وسائل التواصل الاجتماعي. ومع أن المواقع لم تكن مرتبطة بالحملة الأولى، إلا أنها كانت تسعى أيضًا إلى التأثير على الرأي العالمي فيما يخص بابوا الغربية، وتستهدف بالتحديد الجماهير في نيوزلندا وأستراليا.

وقد تمكنا من تحديد الشخص الذي يدير هذه المواقع عبر صفحة على فيسبوك لعلامة تجارية تدعى"Wawawa Journal"، مع أن الاسم السابق للصفحة كان "Tell the Truth NZ"؛ إذ تتيح فيسبوك النظر في تاريخ اسم الصفحة في حال جرى عليه أي تغيير.

وعبر هذا الاسم القديم للصفحة وصلنا إلى اسم النطاق tellthetruth-nz.com، والذي كان مسجلًا باسم محمد روسيد جازولي (Muhamad Rosyid Jazuli).



وعند التواصل معه من طرف صحفيين من بي بي سي، اعترف جازولي بأنه من يدير الحملة، وذكر أنه يعمل مع (Jenggala Center)، وهي مؤسسة أنشأها نائب الرئيس الإندونيسي يوسف كالا (Jusuf

Kalla) عـام 2014؛ بهـدف الترويـج لإعـادة انتخابـه ودعـم إدارة الرئيـس جوكو ويدودو.

يثبـت هـذا التحقيـق أن الكشـف عـن عمليـات التلاعـب والتضليـل وتحديـد الأطـراف المسـؤولة عنهـا مـن أفـراد أو مجموعـات لا يتطلـب بالضـرورة اسـتخدام أسـاليب أو أدوات معقـدة، وإنمـا يتطلـب أحيانًـا بعـض التـروّي، وقليلًا من الحظ.

لقد اعتمـد هـذا التحقيقـات علـى مصـادر مفتوحـة، مثـل بيانـات تسـجيل أسـماء النطـاق للمواقـع الإلكترونيـة، والبحـث العكسـي عـن الصـور، وتحليـل الحسـابات علـى منصـات التواصـل الاجتماعـي والنظـر فـي الكـود المصـدر للمواقع الإلكترونية.

وممّـا سـاعدنا فـي هـذه الحالـة علـى الربـط بيـن الأدلـة للوصـول إلـى النتيجـة النهائية الواضحة هو أن الحملة كانت تعمل على أكثر من منصّة.

كمـا أننـا اسـتفدنا مـن البحـث فـي حسـابات موظفـي شـركة InsightID علـى منصـات التواصـل الاجتماعـي ولينكـد إن، وذلـك مـن الـدروس الأساسـية فـي هـذا المثـال، حيـث تمـت الاسـتفادة مـن التفاصيـل الخاصـة بالحسـابات مـن إحدى المنصّات للتوصّل إلى المزيد من المعلومات في منصّات أخرى.


European
Journalism
Centre


معهد
الجزيرة للإعلام